ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Newman
Escuela de Posgrado

“ Propuesta de mejora de seguridad de la Información digital a desarrollarse en el centro de mediación Online Dispute Resolution Quito - Rumipamba, Ecuador ”

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autor:
Ing. Cando Cando, Edwin Daniel

Docente Guía:
Ing. Honores Incio, Mónica

TACNA – PERÚ
2023

Propuesta de mejora de seguridad de la Información digital a desarrollarse en el centro de mediación Online Dispute Resolution Quito - Rumipamba, Ecuador

ORIGINALITY REPORT

21%	19%	4%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajoson de exclusiva responsabilidad del (los) autor (es)”

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

Este estudio de investigación, se enfocó en optimizar el manejo de la seguridad de la información digital que se genera en el Centro de Mediación Quito-Rumipamba, ubicado en la ciudad de Quito, Ecuador. Para este efecto, se llevó a cabo un diseño detallado que incluyó el análisis de las áreas de vulnerabilidad en la seguridad Informática de este Centro de Mediación.

El procedimiento implicó una evaluación exhaustiva de las prácticas de seguridad existentes en este centro, así como la identificación de posibles amenazas y riesgos en su entorno digital. Se utilizaron distintos instrumentos de recopilación de datos, análisis de archivos y evaluaciones del entorno específico del Centro de Mediación Quito-Rumipamba.

Los resultados revelaron una serie de deficiencias en el manejo de la seguridad de la información en este centro en particular, destacando áreas críticas de mejora en la gestión de accesos, actualizaciones, parches de seguridad y concienciación del personal específico de este centro. Como conclusión, se propuso un conjunto integral de mejores prácticas diseñadas específicamente para abordar estas vulnerabilidades y fortalecer la seguridad en el entorno digital del Centro de Mediación Quito-Rumipamba, la propuesta buscó garantizar la confidencialidad y confiabilidad de los datos, así como la continuidad efectiva de los procesos de mediación de manera ONLINE.

PALABRAS CLAVE: Tesis, Prevención de pérdida de datos (DLP), Seguridad de la Información, Seguridad de Datos

SUMMARY

This research study focused on optimizing the management of the security of digital information generated at the Quito-Rumipamba Mediation Center, located in the city of Quito, Ecuador. For this purpose, a detailed design was carried out that included the analysis of the areas of vulnerability in the IT security of this Mediation Center.

The procedure involved a thorough evaluation of the existing security practices at this center, as well as the identification of possible threats and risks in its digital environment. Different data collection instruments, file analysis and evaluations of the specific environment of the Rumipamba Mediation Center were used.

The results revealed a number of deficiencies in the management of information security at this particular center, highlighting critical areas of improvement in access management, updates, security patches, and staff awareness specific to this center. In conclusion, a comprehensive set of best practices designed specifically to address these vulnerabilities and strengthen security in the digital environment of the Quito-Rumipamba Mediation Center was proposed. The proposal sought to guarantee the confidentiality and reliability of the data, as well as the effective continuity of mediation processes ONLINE.

KEYWORDS: Thesis, Data loss prevention (DLP), Information security, Data security

INTRODUCCION

En la era digital, la resolución de disputas en línea (Online Dispute Resolution - ODR), ha adquirido una creciente relevancia debido a su eficiencia, accesibilidad y conveniencia. Los centros de mediación en línea ofrecen a las partes involucradas en conflictos la oportunidad de resolver sus diferencias de manera virtual, sin tener que recurrir a procesos legales más costosos y prolongados. Sin embargo, esta transformación hacia la mediación en línea también plantea desafíos relacionados con la seguridad de la información digital.

El Centro de Mediación Quito-Rumipamba, brinda servicios online, por lo que necesita que se ponga especial cuidado en la protección de sus datos, a fin de salvaguardarlos de manera efectiva y mantener la confidencialidad de los mismos, ya que como conocemos en los últimos cinco años en Ecuador, varias entidades financieras, de telecomunicaciones, etc. sufrieron ataques a sus sistemas de información digital, causando enormes perjuicios tanto a las empresas como a sus usuarios de sus servicios, por lo cual esta entidad no estaría exenta de ataques informáticos.

En ese contexto, existía una creciente preocupación en el Centro de Mediación Quito-Rumipamba, con respecto a salvaguardar la seguridad de su información digital, ya que se generaron problemas anteriores que pusieron en evidencia las vulnerabilidades en sus sistemas informáticos, y esto amenazaba la confianza, la integridad y la confidencialidad de la información digital de los clientes del centro de Mediación. Por lo cual se acentuaba la necesidad de implementar una solución con urgencia.

Así es como comenzó nuestra investigación para la propuesta de mejoras. En el primer capítulo de este trabajo, se profundiza en los antecedentes que han motivado la necesidad de mejorar la seguridad de datos en el centro de mediación. Aquí, se establecen objetivos claros, como salvar la información y preservar la confianza de todas las partes involucradas.

El segundo capítulo, el Marco Teórico, nos adentra en conceptos fundamentales relacionados con la seguridad de datos, explicando en detalle ¿qué es? y ¿por qué? resulta esencial en la actualidad implementar los sistemas informáticos con las seguridades necesarias para quienes recurren al centro de mediación. Además, se exploran soluciones modernas como BaaS (Backup as a Service) y DRaaS (Disaster Recovery as a Service) para garantizar la protección de los datos.

Avanzando al tercer capítulo, el Marco Referencial, se ofrece una visión completa de la estructura y el funcionamiento de los centros de mediación, sus productos, servicios y, se hace una referencia rápida a la legislación de protección de datos en Ecuador.

En el cuarto capítulo, Resultados, se realiza la Propuesta de Mejora, donde se presenta la parte central de nuestra estrategia, basada en un diagnóstico exhaustivo y un diseño detallado. Aquí, se propone medidas concretas para asegurar los datos, como la implementación de BaaS para la protección de archivos individuales y la adopción de DRaaS para la recuperación integral del sistema en situaciones adversas.

El quinto y último capítulo resumen las conclusiones y recomendaciones derivadas de nuestra propuesta. Se argumenta el ¿porqué? BaaS y DRaaS se perfilan como

opciones sólidas para mejorar la seguridad y se proporcionan orientaciones prácticas para su implementación efectiva.

Finalmente, la bibliografía y los anexos respaldan rigurosamente este estudio, consolidando una propuesta integral para elevar los estándares de seguridad de la información en los centros de mediación.

.

CAPITULO I: ANTECEDENTES DEL ESTUDIO

1.1. Título del Tema: “Propuesta de mejora de seguridad de la Información digital a desarrollarse en el centro de mediación Online Dispute Resolution Quito- Rumipamba, Ecuador”

1.2. Planteamiento del Problema:

La problemática en el Centro de Mediación Quito-Rumipamba se centra en la vulnerabilidad de la seguridad de la información. La variable dependiente en esta situación es la seguridad de los datos y la confianza de las partes involucradas en el proceso de mediación en línea.

La variable independiente que ha dado origen a esta problemática es la falta de medidas adecuadas de seguridad de la información. Los sistemas existentes no ofrecen la protección necesaria contra amenazas cibernéticas, lo que ha llevado a una preocupación creciente entre los usuarios.

Si esta situación no se resuelve o mejora, la variable dependiente, es decir, la seguridad de la información, seguirá siendo vulnerable a ataques y violaciones de datos. Esto resulta en la pérdida de la confianza de los clientes y partes involucradas en el proceso de mediación, lo cual puede ocasionar pérdidas materiales y económicas de los usuarios, lo que a su vez afectaría negativamente la reputación y la efectividad del centro de mediación Quito-Rumipamba.

Es crucial llevar a cabo un estudio explicativo en esta situación para comprender por qué la seguridad de la información es un elemento esencial en los procesos de

mediación en línea y por qué su vulnerabilidad puede tener repercusiones significativas. La importancia de este estudio radica en la necesidad de identificar soluciones efectivas que protejan los datos y, al mismo tiempo, mantener la confianza de quienes utilizan los servicios de mediación en línea.

1.3. Objetivos de la Investigación

1.3.1. Objetivo General:

Mejorar la seguridad de la información digital en el Centro de Mediación Quito-Rumipamba de Quito, Ecuador, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos utilizados en procesos de mediación en línea.

1.3.2. Objetivos Específicos:

1.3.2.1 Realizar un diagnóstico de la situación actual en el centro de mediación Rumipamba - Quito.

1.3.2.2. Identificar las vulnerabilidades y riesgos asociados a la seguridad de la información en este centro.

1.3.2.3. Diseñar medidas y prácticas de seguridad para fortalecer la protección de la información digital.

1.3.2.4. Recomendar mecanismos de control para evaluar la efectividad de las mejoras sugeridas.

1.4. Metodología:

La metodología de esta investigación se basará en un enfoque mixto, utilizando tanto métodos cuantitativos como cualitativos. Se realizará un análisis de la situación actual de los sistemas de seguridad de la información mediante la recopilación de datos cuantitativos y evaluación de la infraestructura tecnológica.

Además, se llevarán a cabo investigaciones con expertos en mediación y seguridad de la información para obtener información cualitativa sobre los desafíos y las mejores prácticas. Los datos recopilados se analizarán de manera integrada para identificar las vulnerabilidades y proponer mejoras.

A fin de dar cumplimiento a cada uno de los objetivos se seguirá la siguiente metodología por cada objetivo.

Diagnóstico de la Situación Actual: Para cumplir con el objetivo de diagnosticar la situación actual, se llevará a cabo una evaluación cuantitativa utilizando herramientas automatizadas como Nmap o Nessus para la evaluación de vulnerabilidades de la red y un enfoque cualitativo mediante reuniones con el personal. Este enfoque integral permitirá una comprensión completa de la situación actual.

Identificación de Vulnerabilidades: La identificación de vulnerabilidades se llevará a cabo mediante métodos cuantitativos, como el análisis de datos y métodos cualitativos, a través de reuniones con el personal enfocado en identificar riesgos específicos, documentos que deben ser protegidos, etc.

Diseño de Medidas de Seguridad: El diseño de medidas de seguridad se basará en investigaciones cuantitativas y cualitativas para garantizar la idoneidad de las soluciones y su alineación con la cultura organizacional.

Recomendar Mecanismos de Control: La evaluación de la efectividad de las medidas de seguridad se realizará cuantitativamente mediante métricas clave y cualitativamente a través de entrevistas con el personal. Esto proporcionará una visión integral de la efectividad de las mejoras implementadas

1.4.1. Tipo y diseño de la Investigación

El tipo de investigación utilizado en este estudio es de carácter aplicado, ya que busca resolver un problema práctico en un contexto específico. Además, se utiliza un enfoque de estudio de caso para analizar en detalle la seguridad de la información en el centro de mediación en línea ODR-Quito-Rumipamba, Ecuador. Y de manera particular en el centro de mediación Quito- Rumipamba. Este enfoque permitirá obtener información detallada y contextualizada sobre las prácticas existentes y los desafíos relacionados con la seguridad de la información.

1.4.2. Fases de la Investigación

El estudio se llevará a cabo en tres fases principales: planificación, ejecución y publicación de resultados.

1.4.2.1. Planificación

Durante la fase de planificación, se establecerán los objetivos de identificar las principales vulnerabilidades de seguridad en el centro de mediación en línea y proponer medidas de mejora. Además, se utilizarán herramientas técnicas como el marco teórico para establecer un marco de referencia para la evaluación y mejora de la seguridad. Esto ayudará a fundamentar teóricamente la investigación y a identificar posibles enfoques y mejores prácticas que se pueden aplicar.

1.4.2.2. Ejecución

En esta fase, se llevarán a cabo las actividades de recolección de datos, como la aplicación de cuestionarios, las entrevistas y el análisis de documentos. También se realizarán análisis de seguridad para identificar posibles vulnerabilidades y brechas en los sistemas de información del centro de mediación.

Durante la fase de ejecución, se utilizarán herramientas técnicas que permitirán identificar posibles puntos débiles en la infraestructura de TI y proporcionarán información valiosa para la mejora de la seguridad de la información.

1.4.2.3. Publicación de Resultados

La publicación de resultados se realizará en forma de un informe detallado que incluirá los resultados del análisis de datos, las conclusiones obtenidas y las recomendaciones específicas para mejorar la seguridad de la información en el centro de mediación en línea. Además, se buscará la presentación de los resultados en conferencias para el resto de centros de mediación en línea a nivel internacional, para compartir el

conocimiento adquirido y fomentar la discusión y el avance en el ámbito de la seguridad de la información.

1.5. Justificación:

En el Centro de Mediación Quito-Rumipamba, se ha identificado una preocupante vulnerabilidad en la seguridad de la información. Este problema es crucial, ya que compromete la confidencialidad e integridad de los datos manejados en un entorno que requiere una protección meticulosa. La revisión de literatura y análisis previos ha confirmado que existe una brecha significativa en la investigación sobre seguridad en centros de mediación, subrayando la necesidad urgente de abordar esta problemática.

Esta investigación se relaciona directamente con la teoría y conocimiento existente en campos como la ciberseguridad y la gestión de datos en línea. Contribuirá al conocimiento al explorar nuevas estrategias y enfoques para fortalecer la seguridad de la información en un contexto específico de mediación en línea. La investigación busca llenar una brecha de conocimiento identificada en este campo, proporcionando una perspectiva única y valiosa.

Desde un punto de vista práctico, esta investigación tiene aplicaciones concretas y beneficios tangibles. Mejorar la seguridad de la información en el Centro de Mediación Quito-Rumipamba no solo preserva la integridad de los datos de las partes involucradas, sino que también tiene un impacto positivo en la eficacia y confiabilidad de los procesos de mediación en línea. Los resultados de este estudio no solo serán académicamente valiosos, sino que también ofrecerán directrices prácticas para

fortalecer la seguridad de datos en situaciones similares, teniendo una influencia positiva en la toma de decisiones y la gestión de la información.

En resumen, esta investigación es esencial debido a la problemática identificada en el Centro de Mediación Quito-Rumipamba. Su relevancia teórica y práctica la posiciona como un proyecto valioso que contribuirá tanto al conocimiento académico como a la mejora de las prácticas en el ámbito de la seguridad de la información en centros de mediación en línea

1.6. Principales Definiciones:

Sistema de seguridad de la información digital: Conjunto de políticas, procedimientos y tecnologías utilizados para proteger la confidencialidad, integridad y disponibilidad de la información digital en los centros de mediación en línea.

Centros de mediación de resolución de disputas en línea: Plataformas digitales que facilitan la resolución de conflictos entre las partes involucradas mediante el uso de medios físicos, electrónicos y herramientas de comunicación en línea.

Online Dispute Resolution: O.D.R. Resolución de Disputas en Línea.

Seguridad de Datos: Medidas y prácticas implementadas para proteger la información digital contra accesos no autorizados, daños o pérdidas.

Confidencialidad: Garantía de que la información solo es accesible para las personas autorizadas y no se comparte con personas no autorizadas.

BaaS (Backup as a Service): Solución tecnológica que permite hacer copias de seguridad regulares de los datos y guardarlas en un lugar seguro, para su recuperación en caso de pérdida o daño.

DRaaS (Disaster Recovery as a Service): Enfoque que asegura la continuidad operativa restaurando sistemas y datos después de un fallo grave o desastre.

Vulnerabilidad: Punto débil en la seguridad que podría ser explotado por ciberataques o eventos adversos.

Riesgo: Probabilidad de que una vulnerabilidad se materialice, causando daño o pérdida.

Integridad de Datos: Garantía de que la información no ha sido alterada o manipulada de manera no autorizada.

Confianza del Usuario: La seguridad y la protección de la información fomentan la confianza en la organización y sus servicios.

Implementación: Acción de llevar a cabo soluciones propuestas para mejorar la seguridad.

Evaluación de Riesgos: Proceso de identificar y medir los posibles riesgos asociados con la seguridad de datos.

Factibilidad: Análisis de si las soluciones propuestas son viables y pueden ser implementadas con recursos disponibles.

Costo/Beneficio: Evaluación de los gastos frente a los beneficios potenciales de la implementación de soluciones de seguridad.

Infraestructura Actual: Los sistemas, tecnologías y prácticas de seguridad ya en uso en el centro de mediación.

Continuidad Operativa: Capacidad de mantener la funcionalidad incluso después de un fallo grave o desastre.

Efectividad: Evaluar cómo las soluciones implementadas logran los objetivos de seguridad y protección de datos.

1.7. Alcances y Limitaciones:

1.7.1. Alcance

El alcance de la propuesta de mejora en los sistemas de seguridad de la información digital en los centros de mediación de resolución de disputas en línea en Quito, en particular del centro de mediación Rumipamba, debe abarcar lo siguiente:

Diagnóstico de Seguridad: Realizar un análisis exhaustivo de la situación actual de los sistemas de seguridad utilizados en los centros de mediación, identificando fortalezas y debilidades.

Identificación de Vulnerabilidades: Detectar y evaluar las vulnerabilidades y riesgos asociados a la seguridad de la información en estos centros, tanto a nivel de infraestructura como de procesos.

Diseño de Medidas de Seguridad: Proponer medidas y prácticas de seguridad adecuadas y eficientes para fortalecer la protección de la información digital de las partes involucradas en el proceso de mediación.

Recomendaciones de Control: Sugerir mecanismos de control que permitan evaluar la efectividad de las mejoras implementadas y garantizar el cumplimiento de las políticas de seguridad.

1.7.2. Limitaciones

Esta investigación se limitará a los centros de mediación de resolución de disputas en línea ubicados en la ciudad de Quito, Ecuador. En particular al Centro de mediación ODR Quito-Rumipamba, que es el que coordina a los demás centros de mediación de la Provincia de Pichincha, debido a restricciones de tiempo y recursos financieros, no se incluirán otros centros de mediación ubicados en diferentes ciudades del país. Además, las recomendaciones propuestas estarán sujetas a la viabilidad y factibilidad de implementación por parte de los centros de mediación, tanto desde el punto de vista tecnológico como económico.

Es esencial tener en cuenta tanto el alcance como las limitaciones de la propuesta de mejora para asegurar una implementación exitosa y realista. La gestión adecuada de estas consideraciones permitirá lograr mejoras significativas en la seguridad de la información del centro de mediación y proporcionar un entorno seguro y confiable para todas las partes involucradas

CAPITULO II: MARCO TEORICO

Dado que el presente estudio se realiza para proteger la información digital de un centro de mediación, es importante se defina con claridad ¿Qué entendemos por “seguridad de datos informáticos”?, ¿Cuáles son sus principales componentes y su importancia, en el contexto de los centros de mediación en línea?, etc.

2.1. Conceptualización de la(s) variable(s) o tópico(s) clave

A continuación se definen algunos conceptos claves, principios y se explica con mayor detalle cada una de las amenazas a las que esta expuesto el centro de mediación, lo cual ratifica la importancia del presente estudio.

Definición de Seguridad de la Información:

La seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas y recursos relacionados. Se trata de salvaguardar la información contra amenazas y riesgos, garantizando que solo las personas autorizadas tengan acceso a ella y que no se vea comprometida ni alterada de manera no autorizada.

En el contexto de este proyecto, se abordará la conceptualización de las variables clave relacionadas con la Seguridad de la Información en el Centro de Mediación Quito-Rumipamba, que son:

Integridad de la Información: La integridad se refiere a la precisión y confiabilidad de la información. Los datos deben mantenerse libres de alteraciones no autorizadas o manipulaciones.

La integridad asegura que la información en el centro de mediación sea precisa y no esté sujeta a cambios maliciosos, garantizando la validez y la confianza en los datos utilizados durante los procesos de mediación.

Confidencialidad de la Información: La confidencialidad implica que la información solo está disponible para aquellos autorizados a acceder a ella. Se busca evitar la divulgación no autorizada de datos sensibles.

Dado que el centro de mediación maneja información altamente confidencial sobre disputas y acuerdos, la confidencialidad es esencial para mantener la privacidad de las partes involucradas.

Disponibilidad de la Información: La disponibilidad se refiere a la accesibilidad de la información cuando sea necesario. Implica garantizar que la información esté disponible y accesible para los usuarios autorizados.

Importancia: La información debe estar disponible para facilitar un proceso de mediación efectivo. La falta de disponibilidad podría afectar negativamente la toma de decisiones y la eficiencia del centro.

Gestión de Riesgos en la Seguridad de la Información: La gestión de riesgos implica la identificación, evaluación y mitigación de posibles amenazas a la seguridad de la información.

En un entorno digital, la gestión de riesgos es fundamental para anticipar y abordar posibles amenazas a la seguridad de los datos en el centro de mediación.

En conjunto, estas variables constituyen la base para diseñar un sistema de seguridad de la información robusto y efectivo en el contexto del Centro de Mediación Rumipamba. Cada una juega un papel crucial en la protección y preservación de la integridad, confidencialidad y disponibilidad de la información durante los procesos de mediación.

Figura 1

Protección de Datos en entornos digitales, Ciberseguridad

Nota. La imagen proporciona una representación visual de la ciberseguridad en la red de datos.

Fuente: Pixabay (2023). Recuperado de https://pixabay.com/es/vectors/la-ciberseguridad-cerrar-con-llave-6673412/

En el contexto de los centros de mediación en línea, la seguridad de la información implica asegurar que los datos personales y los detalles de las disputas sean tratados de manera confidencial y estén protegidos contra accesos no autorizados. Esto puede incluir medidas como la encriptación de datos, el establecimiento de políticas de acceso y el uso de sistemas de autenticación para garantizar que solo las partes involucradas y el mediador tengan acceso a la información relevante.

2.2. Importancia de Seguridad de la Información en entornos Digitales:

La importancia de la seguridad de la información en entornos digitales radica en la creciente dependencia de las organizaciones y los individuos en la tecnología y la información digital. Los entornos digitales son propensos a amenazas y riesgos, como el acceso no autorizado, la manipulación de datos y los ataques cibernéticos, que pueden tener consecuencias graves, incluida la pérdida de datos, la violación de la privacidad y la interrupción de las operaciones.

En los centros de mediación en línea, la importancia de la seguridad de la información se destaca debido a la confidencialidad requerida en el manejo de disputas. Si los datos de las partes involucradas se ven comprometidos, podría haber consecuencias legales, pérdida de confianza de los clientes y daño a la reputación del centro de mediación.

2.2.1. Principios de: Confidencialidad, integridad y disponibilidad:

La tríada CID, compuesta por los principios de Confidencialidad, Integridad y Disponibilidad, es un conjunto de conceptos fundamentales en el ámbito de la seguridad de la información. Estos principios se utilizan para garantizar la protección y el adecuado manejo de los datos y sistemas en entornos digitales.

Es importante destacar que estos principios no son independientes y se complementan entre sí. Para lograr una seguridad efectiva, es necesario considerar y aplicar los tres principios en conjunto. Además, otros principios, como la autenticidad, la trazabilidad y la no repudiación, también pueden estar vinculados a la tríada CID en el contexto de la seguridad de la información.

Figura 2

Confidencialidad, Integridad y Disponibilidad de la Información

Nota. El gráfico ilustra los tres elementos fundamentales de la seguridad de la información. Tomado del artículo "Confidencialidad, Integridad y Disponibilidad" de autoría de Carlos A.

Martinez Ramirez, 2023, https://www.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez/?originalSubdomain=es

Confidencialidad: Este principio implica garantizar que la información solo esté accesible para las personas autorizadas. Se deben establecer controles y medidas de seguridad para proteger la información sensible contra accesos no autorizados.

En un centro de mediación en línea, se puede implementar el cifrado de datos para proteger la confidencialidad de la información transmitida entre las partes involucradas y el mediador. Esto garantiza que solo las partes autorizadas puedan acceder a la información y comprender los detalles de la disputa.

Integridad: La integridad se refiere a la precisión y consistencia de la información a lo largo de su ciclo de vida. Se busca evitar cualquier modificación no autorizada o no intencionada de la información.

En un centro de mediación en línea, se pueden implementar mecanismos de control de versiones y registros de auditoría para asegurar que los acuerdos y documentos relacionados con la mediación no sean modificados sin autorización. Esto garantiza que la información se mantenga íntegra y no se vea comprometida.

Disponibilidad: La disponibilidad se refiere a garantizar que la información y los recursos estén disponibles cuando se necesiten. Esto implica evitar interrupciones no planificadas y asegurar una infraestructura confiable.

En un centro de mediación en línea, se deben implementar medidas para garantizar la disponibilidad continua de la plataforma y los sistemas utilizados para llevar a cabo la

mediación. Esto implica tener copias de seguridad periódicas, sistemas de respaldo y redundancia en caso de fallas.

2.2.2.Gestión de riesgo de la seguridad informática:

La gestión de riesgos de la seguridad informática se refiere al proceso de identificar, evaluar y mitigar los riesgos asociados con la seguridad de la información y los sistemas informáticos. Consiste en analizar las posibles amenazas y vulnerabilidades, determinar el impacto potencial de los riesgos y aplicar medidas para reducir o eliminar dichos riesgos.

En el contexto de los centros de mediación en línea, la gestión de riesgos de seguridad informática implica identificar posibles vulnerabilidades en la plataforma y los sistemas tecnologicos utilizados para la mediación. Esto puede incluir el análisis de riesgos como el acceso no autorizado a los datos de las partes involucradas, el compromiso de la integridad de los documentos de mediación o la interrupción del servicio debido a ataques cibernéticos. Con base en este análisis, se pueden implementar controles y medidas de seguridad adecuados, como firewalls, sistemas de detección de intrusiones y políticas de seguridad, para mitigar los riesgos identificados.

2.2.3. Amenazas en entornos digitales:

Las amenazas en entornos digitales son situaciones o eventos que pueden comprometer la seguridad de la información y los sistemas informáticos. Estas

amenazas pueden venir tanto de fuentes internas como externas, incluyendo actividades maliciosas, errores humanos, desastres naturales y fallas técnicas.

Algunas amenazas comunes en los centros de mediación en línea pueden ser el acceso no autorizado a los datos de las partes involucradas, el robo de información confidencial, la interceptación de comunicaciones, el malware y los ataques de denegación de servicio. Estas amenazas posiblemente tendrán un impacto significativo en la confidencialidad, integridad y disponibilidad de la información de mediación, y deben abordarse mediante medidas de seguridad adecuadas.

2.2.4 Ataques de Hacker:

Los ataques de hacker son intentos maliciosos de acceder, manipular o dañar sistemas informáticos, redes o datos de manera no autorizada. Los hackers utilizan diversas técnicas y herramientas para aprovechar las vulnerabilidades de seguridad y obtener acceso no autorizado a la información o sistemas protegidos.

Figura 3

Ciberseguridad: Hacker de internet

Nota. El gráfico es una representación visual de las distintas formas de ataque de un Hacker, Fuente: Pixabay (2023), https://pixabay.com/es/vectors/la-ciberseguridad-6949298/

En el contexto de los centros de mediación en línea, un ataque de hacker puede ser un intento de obtener acceso no autorizado a los datos, actas y documentos de las partes involucradas en la mediación. Esto podría involucrar técnicas como la ingeniería social, el phishing o la explotación de vulnerabilidades en la plataforma o en los sistemas utilizados. Los ataques de hacker pueden resultar en la divulgación de información confidencial, la alteración de los acuerdos de mediación o la interrupción del servicio, lo cual pone en riesgo la integridad y la confidencialidad de la información.

2.2.5 Virus Informático:

Un virus informático es un programa o código malicioso diseñado para replicarse y propagarse de un sistema a otro, con el objetivo de dañar, alterar o robar información. Los virus informáticos pueden infectar archivos, programas o incluso sectores de inicio en un dispositivo o red.

En el contexto de los centros de mediación en línea, un virus informático puede infectar los sistemas utilizados para almacenar y procesar la información de mediación. Por ejemplo, un virus puede propagarse a través de un archivo adjunto malicioso en un correo electrónico enviado a las partes involucradas en la mediación. Una vez que el archivo se abre, el virus se activa y puede dañar los datos, comprometer la seguridad de la información o incluso bloquear el acceso a los sistemas. La detección y eliminación de virus informáticos requiere el uso de software de seguridad actualizado y

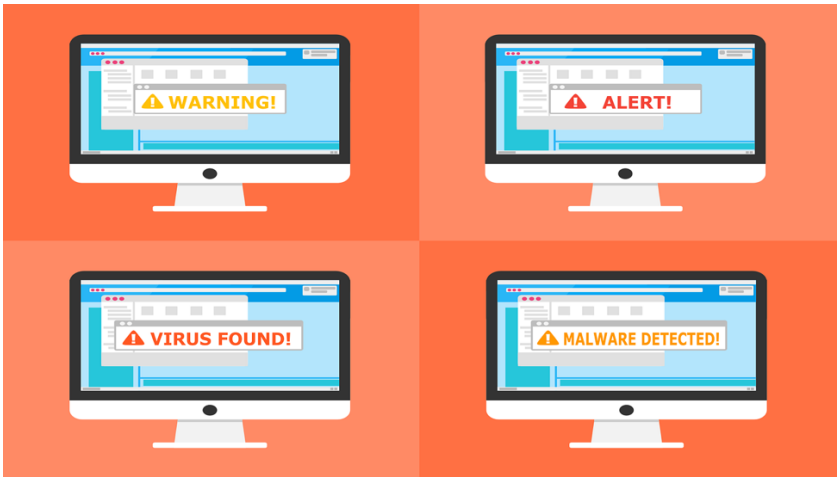
medidas de prevención, como evitar abrir archivos adjuntos sospechosos o descargar software de fuentes no confiables.

2.2.6. Malware:

El malware es un término general que se refiere a software malicioso diseñado para dañar, alterar o acceder de manera no autorizada a sistemas informáticos y redes. Incluye una amplia gama de amenazas, como virus, gusanos, troyanos, ransomware y spyware. El malware puede ingresar a un sistema a través de descargas de archivos infectados, enlaces maliciosos, unidades USB comprometidas, correos electrónicos de phishing y otras técnicas de ingeniería social.

Figura 4

Tipos de Alerta de Virus, malware, etc.



Nota. El gráfico muestra los distintos tipos de Alerta de Virus, Malware, Fuente: Pixabay (2023) [Ilustración]. Recuperado de https://pixabay.com/es/vectors/advertencia-alerta-detectado-2168379/

En el contexto de los centros de mediación en línea, un ejemplo de malware puede ser un ransomware que se propaga a través de un archivo adjunto de correo electrónico aparentemente legítimo. Una vez que el archivo se abre, el ransomware se instala en el sistema y cifra los datos, solicitando un rescate para desbloquearlos. Esto puede poner en peligro la integridad y la disponibilidad de la información de mediación, afectando la continuidad de los procesos de mediación y la confianza de las partes involucradas.

2.2.7.Robo de datos:

El robo de datos se refiere al acto de obtener información confidencial o sensible de manera no autorizada. Los datos robados pueden incluir información personal, datos financieros, secretos comerciales o cualquier otro tipo de información valiosa que pueda ser explotada con fines maliciosos. El robo de datos puede ocurrir a través de ataques informáticos, brechas de seguridad, robo de dispositivos físicos o incluso acciones internas maliciosas.

En un centro de mediación en línea, el robo de datos puede ocurrir si un atacante logra obtener acceso no autorizado a los servidores o bases de datos que almacenan la información de mediación. Esta información puede incluir detalles personales de las partes involucradas, documentos legales confidenciales o acuerdos de mediación. El robo de estos datos puede tener consecuencias graves, como la violación de la privacidad, el uso indebido de la información o incluso la extorsión.

2.2.8 Normas y estándares internacionales de seguridad de datos:

Las normas y estándares internacionales de seguridad de datos son directrices y mejores prácticas establecidas a nivel global para garantizar la protección de la información y los sistemas informáticos. Existen numerosas normas y estándares internacionales que proporcionan pautas y mejores prácticas para la seguridad de la información, como ISO 27001, NIST SP 800-53, PCI DSS, HIPAA, entre otros. Estas normas proporcionan un marco para la implementación de controles de seguridad, la gestión de riesgos y la protección de la privacidad de los datos, cada cual tiene requerimientos técnicos y económicos que se deben analizar para su implementación.

La norma ISO/IEC 27001 es un estándar reconocido a nivel internacional para la gestión de la seguridad de la información. Esta norma establece requisitos y controles que una organización debe implementar para garantizar la confidencialidad, integridad y disponibilidad de la información.

BAAS (Backup as a Service) y DRAAS (Disaster Recovery as a Service) son soluciones que ofrecen servicios de respaldo y recuperación de datos en entornos digitales. Aunque no son normas técnicas propiamente dichas, existen estándares y mejores prácticas asociadas a estas soluciones que pueden guiar su implementación y garantizar su eficacia. A continuación, se presentan algunos ejemplos de normas técnicas y estándares relevantes para BAAS y DRAAS:

ISO/IEC 27001: Esta norma establece los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Si bien no está específicamente enfocada en BAAS y DRAAS, proporciona una base sólida para asegurar la confidencialidad, integridad y disponibilidad de los datos respaldados y recuperados.

ISO/IEC 27031: Esta norma se centra en la preparación para la continuidad del negocio y establece los requisitos para desarrollar y mantener planes de continuidad del negocio y capacidad de respuesta ante incidentes. Es relevante para la implementación de DRAAS, ya que aborda la necesidad de contar con planes de recuperación y respuesta ante desastres.

ISO/IEC 27002: Esta norma proporciona directrices detalladas para establecer controles de seguridad de la información. Contiene un conjunto exhaustivo de controles y prácticas recomendadas que pueden aplicarse tanto a BAAS como a DRAAS para garantizar la seguridad de los datos respaldados y recuperados.

NIST SP 800-30: Esta guía del National Institute of Standards and Technology (NIST) de Estados Unidos proporciona un enfoque detallado para realizar evaluaciones de riesgos. Es útil para identificar los riesgos asociados con la implementación de BAAS y DRAAS y tomar las medidas adecuadas para mitigarlos.

Es importante destacar que cada solución BAAS y DRAAS puede tener sus propias especificaciones y estándares internos. Los proveedores de servicios pueden implementar controles y procesos adicionales para asegurar la calidad y seguridad de sus servicios. Al seleccionar un proveedor de BAAS o DRAAS, es recomendable evaluar si cumplen con las normas y estándares pertinentes, así como su experiencia y reputación en el mercado.

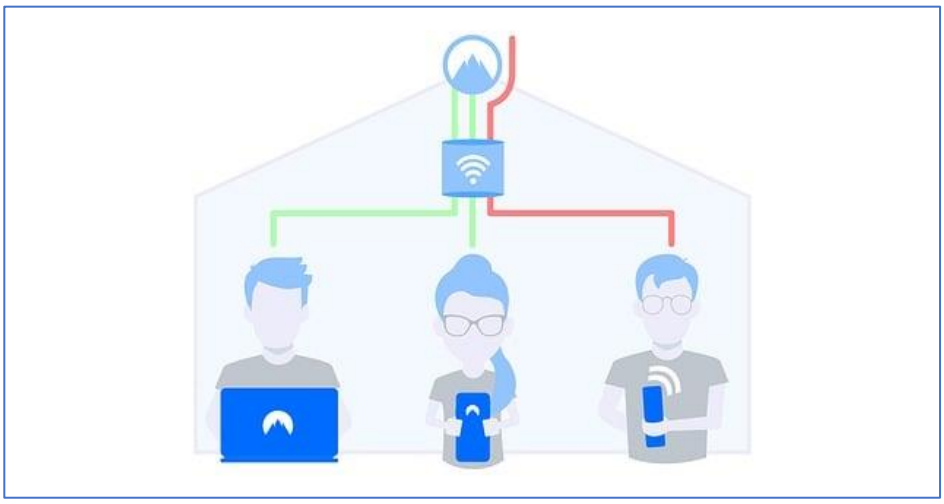
Es fundamental tener en cuenta que las soluciones BAAS y DRAAS son complementarias a las normas y estándares mencionados anteriormente, ya que se centran en la implementación práctica y la entrega de servicios específicos de respaldo y recuperación de datos.

2.2.9. Mejores prácticas para la seguridad en entornos digitales:

Las mejores prácticas para la seguridad de la información en entornos digitales son fundamentales para proteger los sistemas y datos contra amenazas y ataques. Estas prácticas abarcan una amplia gama de áreas, desde la implementación de controles de seguridad hasta la gestión de riesgos y la concienciación del personal.

Figura 5

Formas de Conexión segura (VPN) e insegura hacia la red



Nota. El gráfico muestra la forma en que los usuarios nos conectamos a una red de datos con distintos dispositivos de manera segura a través de una VPN y otros no utilizan nada, Fuente: Pixabay (2023), VPN: Seguridad para el hogar [Ilustración]. Recuperado de https://pixabay.com/es/illustrations/vpn-vpn-de-seguridad-para-el-hogar-4038296/

La implementación de controles de seguridad es esencial para proteger los sistemas y la información en entornos digitales. Algunos ejemplos de controles de seguridad incluyen:

Autenticación sólida:

Utilizar métodos de autenticación robustos, como contraseñas seguras y autenticación de dos factores, para asegurar que solo los usuarios autorizados puedan acceder a los sistemas y datos.

Acceso basado en roles:

Establecer políticas de acceso basadas en roles, lo que significa que los usuarios solo tienen acceso a la información y los recursos necesarios para realizar sus funciones.

Encriptación de datos:

Aplicar técnicas de encriptación para proteger la confidencialidad de los datos, tanto en tránsito como en reposo. Por ejemplo, utilizar protocolos seguros como HTTPS para proteger las comunicaciones en línea.

Gestión de riesgos:

La gestión de riesgos implica identificar, evaluar y mitigar los riesgos asociados con la seguridad de la información. Algunas prácticas clave incluyen:

Evaluación de riesgos:

Realizar evaluaciones periódicas de riesgos para identificar las amenazas y vulnerabilidades que enfrentan los sistemas y los datos. Por ejemplo, realizar análisis de vulnerabilidades y pruebas de penetración para detectar posibles brechas de seguridad.

Plan de respuesta a incidentes:

Establecer un plan de respuesta a incidentes que defina los pasos a seguir en caso de una brecha de seguridad. Esto garantiza una respuesta rápida y efectiva para minimizar el impacto de un incidente.

Actualización y parcheo:

Mantener los sistemas y software actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas. Esto reduce la exposición a ataques que aprovechan vulnerabilidades conocidas.

Concienciación del personal:

La concienciación del personal es crucial para fomentar una cultura de seguridad de la información. Algunas prácticas para lograr esto son:

Programas de formación en seguridad: Implementar programas de formación y capacitación regulares para educar a los mediadores y personal administrativo sobre las mejores prácticas de seguridad, como la identificación de correos electrónicos de phishing, el uso seguro de contraseñas y la protección de datos confidenciales.

Políticas de seguridad:

Establecer políticas claras de seguridad de la información que definan las responsabilidades y las pautas para el uso seguro de los sistemas y datos. Por ejemplo, establecer políticas de uso aceptable de los recursos informáticos y políticas de protección de datos.

Informes de incidentes:

Fomentar una cultura de informes de incidentes, donde los usuarios, mediadores y personal administrativo se sientan seguros y alentados a informar cualquier incidente de seguridad o sospecha de actividad maliciosa.

2.3. Análisis Comparativo BaaS y DRaaS

Análisis Comparativo entre BASS y DRaaS en el Contexto de Mejora en Seguridad de Datos Informáticos

El análisis comparativo entre las soluciones Backup as a Service (BaaS) y Disaster Recovery as a Service (DRaaS) es esencial para determinar cuál de ellas es más adecuada para mejorar la seguridad de datos informáticos en el Centro de Mediación ODR Quito Rumipamba. A continuación, se presenta un análisis detallado junto con ejemplos prácticos:

2.3.1 Backup as a Service (BaaS)

BaaS implica la copia regular y automatizada de datos a un almacenamiento seguro. Permite la recuperación de datos en caso de pérdida, daño o eliminación accidental. Aquí hay un análisis de BaaS:

Ventajas de BaaS:

Recuperación de Datos Rápida: En caso de pérdida de datos, BaaS permite la recuperación rápida y eficiente de los datos respaldados.

Prevención contra Eliminación Accidental: BaaS evita la pérdida de datos debido a eliminaciones accidentales al tener copias de seguridad en un lugar seguro.

Desventajas de BaaS:

No Aborda Interrupciones del Sistema Completo: BaaS no es adecuado para la recuperación de sistemas completos en caso de falla.

Ejemplo Práctico de BaaS: Si un mediador elimina accidentalmente un archivo importante en la plataforma de mediación, el sistema de BaaS puede restaurar ese archivo desde una copia de seguridad reciente.

2.3.2 Disaster Recovery as a Service (DRaaS)

DRaaS es un enfoque más completo que BaaS. Implica replicar de manera continua sistemas completos y datos en un entorno de respaldo. Permite la recuperación rápida de todo el sistema en caso de interrupciones graves.

Ventajas de DRaaS:

Recuperación Completa del Sistema: DRaaS permite la recuperación rápida de todo el sistema, incluidos los sistemas operativos, aplicaciones y datos.

Menos Tiempo de Inactividad: En caso de un fallo grave, DRaaS minimiza el tiempo de inactividad al permitir la recuperación completa en minutos u horas.

Desventajas de DRaaS:

Mayor Complejidad y Costos: DRaaS implica una mayor complejidad técnica y puede tener costos más altos debido a la necesidad de un entorno de respaldo.

Ejemplo Práctico de DRaaS: Si un ataque cibernético compromete el sistema de mediación en línea, DRaaS permitirá la recuperación completa de todo el sistema en un entorno de respaldo.

2.3.3 Comparación y Elección

La elección entre BaaS y DRaaS depende de las necesidades y recursos del Centro de Mediación ODR Rumipamba:

Si se prioriza la recuperación rápida de archivos individuales: BaaS podría ser suficiente para la protección de datos en caso de eliminación accidental o corrupción de archivos.

Si se busca una recuperación completa del sistema en caso de interrupciones graves: DRaaS es la opción preferible, ya que permite la recuperación completa del sistema y minimiza el tiempo de inactividad.

Ejemplo de Elección: Dado que la seguridad de datos es crítica en un centro de mediación, la elección puede inclinarse hacia DRaaS debido a su capacidad para recuperar sistemas completos en situaciones críticas.

Basándonos en el análisis comparativo entre BaaS y DRaaS en el contexto del Centro de Mediación ODR Rumipamba - Quito, podemos extraer las siguientes conclusiones prácticas aplicables:

Implementación de DRaaS para la Recuperación Integral del Sistema : Dado que el Centro de Mediación ODR maneja información sensible y confidencial, la integridad y la disponibilidad del sistema son críticas. Por lo tanto, la implementación de una solución DRaaS sería beneficiosa. En caso de un ataque cibernético grave que cause interrupciones en el sistema, DRaaS permitirá la recuperación completa en un entorno de respaldo, minimizando el tiempo de inactividad y asegurando que el proceso de mediación no se vea afectado negativamente.

Complementario DRaaS con Medidas de BaaS para Recuperación de Datos Individuales : Aunque DRaaS es esencial para la recuperación completa del sistema, no aborda no obstante la recuperación de archivos individuales eliminados accidentalmente. Por lo tanto, sería práctico implementar medidas de BaaS como una capa adicional de protección. Esto garantizará que si un mediador o una parte involucrada elimina accidentalmente un archivo importante, se podrá recuperar rápidamente desde las copias de seguridad de BaaS.

Evaluación de Costos y Recursos : La elección entre DRaaS y BaaS debe considerar los recursos disponibles y los costos asociados. Aunque DRaaS ofrece una

recuperación completa del sistema, puede ser más costoso y complejo de implementar en comparación con otros métodos básicos de almacenamiento en la nube.

2.4 Análisis Crítico BaaS y DraaS

El análisis crítico es esencial para evaluar las implicaciones, ventajas y desventajas de la implementación de soluciones BaaS y DRaaS en el Centro de Mediación ODR Quito Rumipamba. Aquí se examinan los aspectos clave y sus sub-puntos:

2.4.1 Ventajas y Desventajas de BaaS

Ventajas:

Recuperación de Datos Específicos: BaaS permite recuperar datos individuales eliminados o dañados, lo que es útil para casos en los que solo se necesita restaurar archivos específicos.

Sencillez en la Implementación: BaaS es más sencillo de implementar y administrar en comparación con DRaaS. No requiere configuraciones complejas ni un entorno de respaldo.

Desventajas:

Limitaciones en la Recuperación Completa del Sistema: BaaS no aborda la recuperación completa del sistema en caso de falla grave del sistema. No es adecuado para situaciones en las que se requiere una recuperación total.

Ejemplo Práctico de BaaS: Si un mediador elimina accidentalmente un archivo de acuerdo importante, BaaS permite recuperar ese archivo específico sin afectar el funcionamiento general del sistema.

2.4.2 Ventajas y Desventajas de DRaaS

Ventajas:

Recuperación Integral del Sistema: DRaaS permite la recuperación completa del sistema en caso de fallo grave. Esto minimiza el tiempo de inactividad y asegura la continuidad del proceso de mediación.

Mayor Resiliencia ante Interrupciones: DRaaS ofrece una mayor resiliencia ante ataques cibernéticos o fallos del sistema, lo que es fundamental para garantizar la confiabilidad del sistema.

Desventajas:

Complejidad Técnica y Costos: La implementación de DRaaS puede ser más compleja y costosa en términos de configuración y recursos requeridos, sin embargo, en la

práctica, si un ataque cibernético paraliza la plataforma de mediación, DRaaS permite restaurar todo el sistema en un entorno de respaldo, asegurando que las partes involucradas no se vean afectadas y que el proceso de mediación continúe sin problemas.

2.4.3 Evaluación de la Necesidad y los Recursos

Es críterio evaluar las necesidades específicas del Centro de Mediación ODR Quito-Rumipamba, y los recursos disponibles antes de decidir la implementación de BaaS o DRaaS. La elección debe basarse en la importancia de la recuperación de archivos individuales frente a la recuperación completa del sistema, así como en la disposición de recursos financieros y técnicos.

Dado que el centro tiene un equipo de TI limitado y un presupuesto ajustado, se puede considerar implementar BaaS como una medida práctica para garantizar la recuperación de datos individuales importantes, en una primera etapa.

Basándonos en el análisis crítico de la implementación de BaaS y DRaaS en el Centro de Mediación ODR Quito Rumipamba, podemos extraer las siguientes conclusiones prácticas aplicables:

Selección Basada en Infraestructura y Recursos : El análisis destaca que BaaS es más adecuado ya que tiene una infraestructura tecnológica básica establecida y

recursos limitados. Por otro lado, si el centro está dispuesto a invertir en infraestructura y tiene un equipo técnico capacitado, DRaaS podría ser la elección correcta.

Mitigación de Riesgos y Continuidad del Servicio : En términos de mitigación de riesgos y continuidad del servicio, DRaaS sobresale al recuperar una más sólida en caso de interrupciones graves. Por lo tanto dado que el centro valora la seguridad de los datos y la resiliencia ante amenazas cibernéticas, DRaaS sería una opción más adecuada.

Evaluación Financiera y Presupuestaria : El análisis de factibilidad y costos revela que BaaS generalmente tiene costos más bajos, lo que podría ser especialmente mejorado para un centro con limitaciones financieras. La elección entre BaaS y DRaaS debe considerar cuidadosamente la relación entre los costos y los beneficios en función de las restricciones presupuestarias.

En resumen, las conclusiones prácticas derivadas del análisis crítico apuntan a la necesidad de una selección informada basada en la infraestructura y recursos disponibles, la priorización de la mitigación de riesgos y la continuidad del servicio, y la evaluación financiera y presupuestada. La elección entre BaaS y DRaaS debe ajustarse a las necesidades específicas del Centro de Mediación ODR Rumipamba Quito para garantizar una mejora efectiva en la seguridad de datos informáticos.

CAPITULO III: MARCO REFERENCIAL

3.1. Reseña Histórica

3.1.1. La Mediación como parte del sistema de Justicia

La mediación puede desempeñar un papel importante como parte del sistema de justicia, ya que ofrece una alternativa al proceso judicial tradicional. En muchos sistemas legales, la mediación se utiliza como un enfoque complementario para resolver conflictos y evitar la congestión de los tribunales.

Cuando se integra en el sistema de justicia, la mediación tiene como objetivo principal facilitar la resolución de disputas de manera más rápida, eficiente y satisfactoria para las partes involucradas. A diferencia de los tribunales, donde un juez o un jurado toma la decisión final, en la mediación las partes son las protagonistas del proceso y tienen la oportunidad de tomar decisiones conjuntas.

Aquí hay algunas características clave de la mediación como parte de la justicia:

Voluntariedad: La mediación generalmente requiere el consentimiento voluntario de todas las partes involucradas. No se puede obligar a nadie a participar en el proceso de mediación, lo que permite que las personas tengan un mayor control sobre la resolución de su conflicto.

Confidencialidad:

La mediación se basa en la confidencialidad. Las discusiones y la información compartida durante el proceso son estrictamente confidenciales, lo que promueve un

ambiente seguro para que las partes se expresen libremente y explore soluciones sin temor a que sus declaraciones sean utilizadas en su contra posteriormente.

Imparcialidad del mediador:

El mediador es un tercero neutral e imparcial que no toma partido ni ofrece consejos legales a ninguna de las partes. Su función es facilitar la comunicación y el diálogo constructivo entre las partes para que puedan llegar a un acuerdo mutuamente satisfactorio.

Enfoque colaborativo:

A diferencia de un juicio adversarial, donde las partes se enfrentan entre sí, la mediación promueve un enfoque colaborativo. Las partes son alentadas a trabajar juntas, compartir información y buscar soluciones que satisfagan sus intereses y necesidades mutuas.

Flexibilidad:

La mediación permite adaptarse a las necesidades y circunstancias particulares de cada conflicto. El proceso se puede personalizar para abordar temas específicos y permitir que las partes encuentren soluciones creativas y a medida.

Costos y tiempos reducidos:

En comparación con el proceso judicial, la mediación suele ser más rápida y menos costosa. Al evitar largos procedimientos legales y reducir la carga sobre los tribunales, la mediación puede ofrecer una alternativa más eficiente y accesible para resolver disputas.

Es importante tener en cuenta que la mediación no es adecuada para todos los casos y que ciertos tipos de conflictos pueden requerir intervención judicial. Sin embargo, cuando se implementa de manera adecuada y efectiva, la mediación puede ser una valiosa herramienta en el sistema de justicia, brindando a las partes una mayor participación e independencia en la resolución de sus desacuerdos.

3.1.2. La Mediación en Ecuador

En Ecuador, la mediación se ha establecido como un método alternativo de resolución de conflictos reconocido y respaldado por la Constitución de la República del Ecuador, en el Art. 190. En concordancia con el Código Orgánico General de Procesos (COGEP), promulgado en 2015.

La Constitución de la República del Ecuador, reconoce la mediación como un medio efectivo para resolver disputas y promover la justicia restaurativa. Establece que la mediación puede aplicarse en una amplia gama de casos, incluyendo asuntos civiles,

familiares, comerciales, laborales y comunitarios.

El proceso de mediación en Ecuador generalmente es conducido por mediadores certificados y acreditados, quienes actúan como facilitadores imparciales para ayudar a las partes a llegar a un acuerdo mutuamente aceptable. La mediación se rige por los principios de voluntariedad, confidencialidad, imparcialidad y autonomía de las partes.

La Ley de Mediación y Arbitraje de Ecuador, promulgada en 1997 y actualizada en 2014, también respalda la mediación como un medio alternativo para resolver conflictos. Establece los requisitos y estándares para la formación y certificación de mediadores, así como los procedimientos y principios básicos para llevar a cabo una mediación exitosa.

Además, en Ecuador existen instituciones y centros especializados en la mediación, tanto del sector público como privado, que promueven y facilitan la resolución de conflictos a través de este método. Estos centros ofrecen servicios de mediación, capacitación y asesoramiento en todo el país.

La mediación en Ecuador ha demostrado ser una herramienta valiosa para descongestionar los tribunales, promover la participación activa de las partes y buscar soluciones consensuadas. Se considera una opción favorable para resolver disputas de manera más rápida, menos costosa y más satisfactoria para las partes involucradas.

3.2. Filosofía Organizacional

Los Centros de Mediación ODR Ecuador, esta conformado por un equipo de mediadores profesionales multidisciplinarios; entre ellos negociadores, árbitros, con vasta experiencia resolviendo conflictos en vía extrajudicial como judicial.

Al ingresar a la página web de Online Dispute Resolution Ecuador (s.f.) Quiénes somos. Recuperado el 14 de Agosto de 2023, de https://odrecuador.com/quienes-somos, podemos encontrar las pautas principales de su filosofía organizacional:

"**MISION:**

Convertirnos en referentes de la prestación de servicios académicos, formación, arbitraje y mediación a través de nuestra red de Centros.

VISION:

Liderar la oferta de servicios que genera ODR Ecuador a nivel Internacional hasta el 2030.

OBJETIVOS PRINCIPALES:

Promover la utilización de MASC a nuestros clientes y, usuarios a través de la red de Centros ODR-E.

Generar espacios de difusión, capacitación y, trabajo de los servicios que brindamos en ODR-E.

Incentivar la transformación de la sociedad conflictiva a colaborativa, para armonizar la convivencia social y pacífica.

Sus **VALORES** principales son:

Honestidad, Fidelidad, Solidaridad, Confidencialidad, Imparcialidad Y capacidad.”

3.2.1. Centros de Mediación Online Dispute Resolution Ecuador (ODR-E)

Actualmente los centros de Mediación Online Dispute Resolution tienen oficinas dependientes en varios paises de latinoamérica como Colombia, Perú, Venezuela, Argentina, Ecuador, etc.

En Ecuador, los Centros de Mediación Online Dispute Resolution (ODR, por sus siglas en inglés) se han establecido como una alternativa para brindar servicios de mediación de forma virtual. Al momento en el Ecuador existen 65 oficinas dependientes repartidas en todas las provincias del país, con énfasis en las principales ciudades, de las cuales 5 funcionan en la ciudad de Quito. Estos centros utilizan la tecnología y plataformas en línea para facilitar el proceso de mediación a distancia.

Los Centros de ODR en Ecuador están diseñados para abordar las necesidades de resolución de conflictos en un entorno presencial y digital. Estos centros ofrecen una amplia gama de servicios, que incluyen la mediación en asuntos civiles, familiares, comerciales, laborales y otros ámbitos de disputa.

Uno de los beneficios clave de los Centros de ODR es la flexibilidad y accesibilidad que brindan a las partes involucradas. Si bien los servicios de mediación se pueden realizar de manera presencial, dichos servicios se potencializan al utilizar herramientas de comunicación en línea, como videoconferencias y salas virtuales, las partes pueden

participar en el proceso de mediación desde cualquier ubicación geográfica, eliminando las barreras de tiempo y distancia.

Estos centros generalmente cuentan con mediadores capacitados en el manejo de la mediación en línea y en el uso de las plataformas tecnológicas necesarias. Los mediadores se encargan de facilitar el diálogo entre las partes, ayudándoles a identificar sus intereses y buscar soluciones mutuamente aceptables a través de la comunicación virtual.

La utilización de los Centros de ODR en Ecuador ha experimentado un crecimiento significativo en los últimos años, especialmente a raíz de la pandemia de COVID-19. La necesidad de adaptarse a las restricciones de movilidad y distanciamiento social ha impulsado el uso de la mediación en línea como una forma eficiente y segura de resolver conflictos.

Estos centros trabajan en estrecha colaboración con el sistema judicial y otras entidades relevantes para promover la utilización de la mediación como una herramienta eficaz y eficiente.

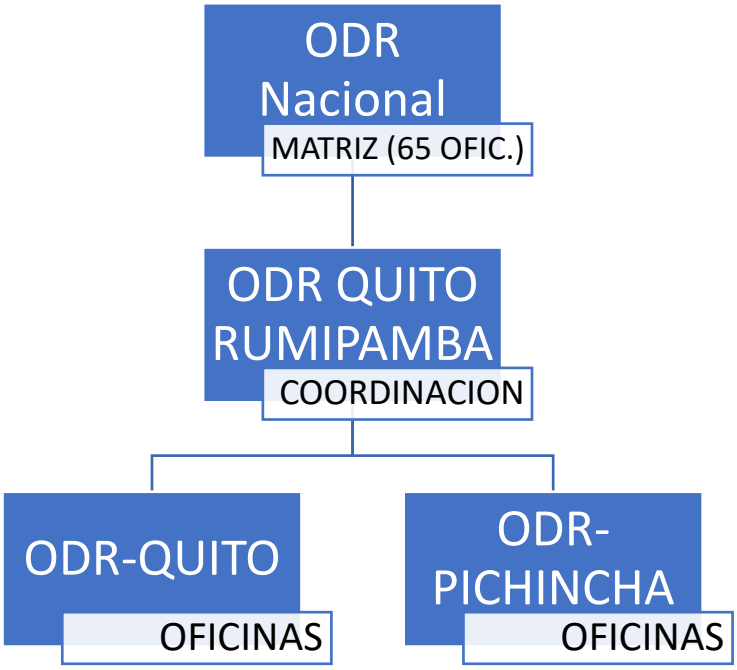
Los Centros de Mediación Online Dispute Resolution en Ecuador brindan una opción conveniente y accesible para que las partes resuelvan sus disputas a través de medios presenciales y/o virtuales. Al combinar la mediación con la tecnología, estos centros ofrecen una alternativa moderna y eficaz para abordar los conflictos y promover la

resolución pacífica de disputas en el entorno digital.

3.3. Diseño Organizacional

FIGURA 6:

DISEÑO ORGANIZACIONAL ODR-ECUADOR OFICINAS DE QUITO Y PICHINCHA



NOTA: La imagen nos muestra el diseño organizacional de ODR-Ecuador en Pichincha,

Fuente: Elaboración propia.

3.3.1. Centro de Mediación Rumipamba - Quito

El "CENTRO DE MEDIACIÓN Y SOLUCIÓN DE CONFLICTOS ONLINE DISPUTE RESOLUTION ECUADOR (ODR-E), oficina dependiente RUMIPAMBA - QUITO, cantón Quito, tiene su domicilio en la ciudad de Quito, provincia de Pichincha, brinda atención en instalaciones propias, ubicado en las calles Av. Rumipamba E2-148 y

Republica, esquina, 4 piso, oficina 401 B, cumple con los requisitos exigidos por el Consejo NacioNl de la Judicatura Ecuatoriano y brinda las facilidades para atender con calidad y calidez a las personas que lo requieran.

Su principal área de influencia comprende el sector CENTRO NORTE del Distrito Metropolitano de Quito, provincia de Pichincha. Población 200.000 personas aproximadamente, y coordina con las demás oficinas de mediación de la provincia de Pichincha que tiene una población de más de 2 millones de habitantes.

Para que un centro de mediación atienda los casos que le llegan, es necesario indicar que existen dos vías para hacerlo; la primera se materializa cuando las instancias judiciales (juzgados y fiscalías) derivan los casos a los centros de mediación ordenado así por ley; y, la segunda vía, opera cuando las personas naturales o jurídicas buscan por su expresa voluntad los centros de mediación.

En relación con los órganos derivantes, se trabajan con los operadores de justicia (jueces y fiscales) en asuntos judicializados en los que las partes tengan el interés de solucionar sus conflictos mediante procesos de mediación.

Por igual, otros actores sociales como profesionales de la abogacía, psicología, trabajo social, ingenieros, arquitectos, líderes políticos y comunitarios, presidentes de comités barriales, miembros de juntas parroquiales, así como, directivos y servidores de empresa privadas, instituciones educativas, de salud, de seguridad ciudadana, como policía nacional, agentes de tránsito, agentes municipales. Dentro de los cultos encontramos a la iglesia Católica y demás grupos religiosos; asociaciones, fundaciones, corporaciones, diversas cámaras; instituciones del Estado, Gobiernos

Autónomos Descentralizados y organizaciones de la sociedad civil, sin olvidar la pequeña y mediana empresa y las instituciones financieras, que por sus particularidades están inmersas en el día a día y son conocedoras e incluso participantes de los diversos problemas que se suscitan en sus espacios y la sociedad, quienes serían potenciales derivadores de conflictos hacia nuestra oficina.

Respecto de las personas naturales o jurídicas, potenciales usuarias del CENTRO DE MEDIACIÓN Y SOLUCIÓN DE CONFLICTOS ONLINE DISPUTE RESOLUTION ECUADOR (ODR-E), oficina dependiente RUMIPAMBA, cantón Quito , atienden a familias, grupos comunitarios, empresas y consumidores de bienes y servicios, instituciones financieras y sus clientes entre otros, en definitiva, a la comunidad en general la cual podrá acudir por las vías antes propuestas, bien por derivación u orientación o bien por solicitud directa.

3.4. Productos y Servicios

Productos y servicios de la mediación presencial:

Sesiones de mediación: Las sesiones de mediación presencial son el servicio principal ofrecido en este formato. Las partes involucradas se reúnen físicamente en un lugar acordado, generalmente con la presencia de un mediador neutral, para discutir y resolver sus diferencias.

Espacios de mediación: Algunos centros de mediación presencial ofrecen espacios especialmente diseñados para llevar a cabo las sesiones de mediación. Estos espacios suelen ser neutral y cómodos, brindando un ambiente propicio para el diálogo y la

colaboración entre las partes.

Servicios de mediación especializada: La mediación presencial ofrece servicios especializados para atender disputas en áreas específicas, como mediación familiar, mediación laboral, mediación comunitaria, mediación penal, entre otros. Estos servicios están adaptados a las necesidades y requerimientos particulares de cada tipo de conflicto.

Asesoramiento y consultoría: Además de las sesiones de mediación, algunos mediadores presenciales también pueden ofrecer servicios de asesoramiento y consultoría juridica antes, durante y después del proceso de mediación. Esto puede incluir orientación sobre estrategias de comunicación, técnicas de resolución de conflictos y asistencia en la redacción de acuerdos.

Productos y servicios de la mediación en línea:

Plataformas de mediación en línea: La mediación en línea se apoya en plataformas digitales diseñadas específicamente para facilitar el proceso de mediación. Estas plataformas ofrecen herramientas de comunicación virtual, como salas de videoconferencia y mensajería instantánea, que permiten a las partes interactuar y colaborar en línea.

Sesiones de mediación virtual: Las sesiones de mediación en línea son el núcleo de los servicios ofrecidos. Las partes se conectan a través de la plataforma en línea y

participan en el proceso de mediación desde la comodidad de sus propias ubicaciones, sin la necesidad de trasladarse físicamente.

Comunicación asistida por tecnología: La mediación en línea incluye servicios y herramientas tecnológicas adicionales para facilitar la comunicación y el intercambio de información entre las partes. Estas herramientas pueden incluyen compartir pantalla, pizarras virtuales y documentos.

Mediación en línea especializada: Al igual que en la mediación presencial, la mediación en línea también ofrece servicios especializados para abordar disputas en áreas específicas, como mediación laboral en línea, mediación familiar en línea, mediación civil y penal en línea, entre otros.

Servicios de asistencia técnica: La mediación en línea requiere un nivel adicional de soporte técnico para garantizar que las partes utilicen la plataforma de manera efectiva. Algunos proveedores de mediación en línea ofrecen servicios de asistencia técnica para solucionar problemas técnicos y brindar orientación durante el proceso.

Es importante tener en cuenta que los productos y servicios varían según el proveedor de mediación y las opciones disponibles en cada contexto específico. Tanto la mediación presencial como la mediación en línea tienen como objetivo principal facilitar la comunicación y promover la resolución pacífica de disputas, empleando diferentes enfoques y herramientas para lograrlo.

3.5. Diagnóstico organizacional o sectorial

En Ecuador, existen diversos centros de mediación, tanto públicos como privados, que brindan servicios de resolución de conflictos a través de la mediación. Estos centros variaan en términos de su estructura, alcance geográfico, especialización y recursos disponibles.

Al realizar un diagnóstico de los centros de mediación en Ecuador, algunos aspectos a considerar podrían ser:

Accesibilidad: Evaluar la accesibilidad de los centros de mediación, tanto en términos geográficos como económicos. ¿Los centros están ubicados estratégicamente para que sean accesibles para las partes involucradas? ¿Los costos de los servicios de mediación son asequibles para la población?

Infraestructura y recursos: Analizar la infraestructura y los recursos disponibles en los centros de mediación. Esto incluye el personal capacitado en mediación, las instalaciones físicas (para que puedan acceder adultos mayores, personas con alguna discapacidad, etc.), las herramientas tecnológicas utilizadas (si ofrecen mediación en línea) y la disponibilidad de materiales y recursos de apoyo.

Capacitación y calidad: Evaluar el nivel de capacitación y competencia de los mediadores en los centros de mediación. ¿Los mediadores cuentan con la formación y

las habilidades necesarias para llevar a cabo un proceso de mediación eficaz? ¿Existe un sistema de evaluación y supervisión de la calidad de los servicios de mediación?

Cobertura y especialización: Analizar la cobertura geográfica de los centros de mediación y su capacidad para atender diferentes tipos de disputas y conflictos. ¿Los centros de mediación cubren todo el territorio nacional o se concentran en áreas específicas? ¿Existen centros especializados en áreas como la mediación familiar, laboral o comunitaria?

Promoción y divulgación: Evaluar las estrategias de promoción y divulgación de los centros de mediación. ¿Los centros de mediación están promoviendo activamente sus servicios y educando a la comunidad sobre los beneficios de la mediación? ¿Existe colaboración con instituciones y organizaciones para difundir la cultura de la resolución pacífica de conflictos?

Marco normativo y apoyo institucional: Analizar el marco normativo y el apoyo institucional existente para los centros de mediación en Ecuador. ¿Existe una legislación clara y actualizada que respalde la mediación? ¿Las instituciones gubernamentales brindan apoyo y reconocimiento a los centros de mediación?

Estos son solo algunos aspectos a considerar al realizar un diagnóstico de los centros de mediación en Ecuador. Cabe destacar que un diagnóstico completo requeriría una investigación más exhaustiva y la recopilación de datos específicos sobre cada centro de mediación en particular.

CAPITULO IV: RESULTADOS

Este capítulo tiene como objetivo principal evidenciar el cumplimiento de los objetivos establecidos en el trabajo de investigación, focalizando en tres aspectos clave: el diagnóstico inicial, el diseño de mejoras propuesto y los mecanismos de control en el Centro de Mediación Rumipamba

4.1. DIAGNÓSTICO

El diagnóstico es una etapa fundamental para identificar las áreas de mejora en la seguridad de datos del centro de mediación. En esta fase, se utilizan diferentes técnicas para:

1. Analizar la infraestructura de seguridad actual,
2. Identificar los datos y aplicaciones críticas para el negocio que deben ser protegidos.
3. Determinar el nivel de protección y recuperación requerido para cada recurso.

Para cumplir con este cometido se utilizarán tablas y formularios que permiten evaluar de manera estructurada las necesidades y requisitos de implementación de DRaaS y BaaS en la empresa, y ayudan a establecer las bases para el diseño y la planificación de la solución.

A continuación, se presenta un paso a paso para implementar DRaaS (Disaster Recovery as a Service) y BaaS (Backup as a Service) en el centro de mediación:

1.- Análisis de la infraestructura de seguridad actual:

El centro de mediación ha identificado la necesidad de mejorar la seguridad de datos para proteger la información sensible de las partes involucradas en los casos de mediación. Se realiza un diagnóstico para evaluar la eficacia del sistema actual de respaldo de datos y la preparación para la recuperación ante desastres, para lo cual se inicia evaluando el estado de la infraestuctura física instalada actualmente.

Tabla 1

Evaluación de la Infraestructura de Seguridad

Aspecto a Evaluar	Descripción	Resultado
Infraestructura de Red	Revisión de la configuración y arquitectura de la red para identificar posibles puntos de vulnerabilidad.	Existe una red tipo LAN y WLAN conectados a un Switch que distribuye el flujo de datos.
Firewall	Evaluación de las políticas de filtrado y reglas del firewall para asegurar que estén adecuadamente configuradas.	No dispone de Firewall local, únicamente el que le proporciona el Internet Server Provider contratado.
Acceso Remoto	Revisión de las conexiones de acceso remoto y de las medidas de autenticación para asegurar la protección de datos.	No existen medidas de autenticación para la protección de datos

Seguridad de Servidores	Análisis de la configuración y parches de seguridad en los servidores para evitar brechas de seguridad.	No se cuenta con servidor propio, aunqe se cuenta con un servicio CLOUD de la plataforma Microsoft.

Fuente: Elaboración Propia

De la evaluación realizada a la infraestructura de red, se encuentra que hay puertos abiertos innecesarios debido a que no se cuenta con un firewall propio, tampoco se utilizan medidas de autenticación, lo que podría ser una puerta de entrada para posibles ataques.

2. Identificar los datos y aplicaciones críticas para el negocio que deben ser protegidos.

En este punto, se identifican los recursos críticos para el negocio, se evalúa su importancia y se determinan los niveles de protección y recuperación requeridos para cada uno. Esto ayuda a priorizar los recursos y definir los objetivos de protección y recuperación.

Tabla 2

Tabla de evaluación de datos y aplicaciones críticas:

Recurso	Importancia para el negocio	Nivel de protección requerido	Nivel de recuperación requerido
Base de datos de clientes	Media	Media	Media
Aplicación de contabilidad	Alta	Alta	Alta
Actas de mediación y sus soportes.	Alta	Alta	Alta
Videos de las sesiones de mediación	Alta	Alta	Alta
Informes de Actas emitidos a la Judicatura	Media	Media	Media

Fuente: Elaboración Propia

3. Determinar el nivel de protección y recuperación requerido para cada recurso.

En esta tabla, se detallan los requisitos específicos de protección y recuperación para un recurso en particular (en este caso, los archivos de diseño). Se establecen criterios como la frecuencia de respaldo, la retención, la ubicación del respaldo, el método de

cifrado, el tiempo objetivo de recuperación (RTO), el punto objetivo de recuperación (RPO) y el proceso de recuperación.

Tabla 3

Formulario de requisitos de protección y recuperación:

	Archivo 1	**Archivo 2**	**Archivo 3**	**Archivo 4**	**Archivo 5**
Recurso:	Base de datos de clientes	Aplicación de contabilidad	Actas de mediación y sus soportes.	Videos de las sesiones de mediación	Informes de Actas emitidos a la Judicatura
Importancia para el negocio:	Media	Alta.	Alta	Alta	Media
Requisitos de protección:					
Frecuencia de respaldo:	Diaria	Diaria	Diaria	Diaria	Semanal

Retención de respaldo:	30 días	60 días	60 días	60	60 días
Ubicación del respaldo:	Almacenamiento en la nube seguro	Almacenamiento en la nube seguro	Almacenamiento en la nube seguro	Almacenamiento en la nube seguro	Almacenamiento en la Nube
Método de cifrado:	AES-256	AES-256	AES-256	AES-256	AES-256
Requisitos de recuperación					
RTO (Objetive Recovery Time)	Menos de 1 hora	Menos de 1 hora	Menos de 1 hora	Menos de 1 hora	Menos de 1 hora
RPO (Objetive Recovery Point)	Menos de 1 hora	Menos de 1 hora	Menos de 1 hora	Menos de 1 hora	Menos de 1 hora
Proceso de	Restauración	Restauración	Restauración	Restauración	Restauración

Recuperación	rápida de archivos desde el almacenamiento de la nube	rápida de archivos desde el almacenamiento de la nube	rápida de archivos desde el almacenamiento de la nube	rápida de archivos desde el almacenamiento de la nube	rápida de archivos desde el almacenamiento de la nube

Fuente: Elaboración Propia

El diagnóstico realizado en el Centro de Mediación Quito-Rumipamba reveló una serie de hallazgos críticos relacionados con la seguridad de la información. Se identificaron vulnerabilidades en la red, acceso no autorizado a archivos, debilidades en los protocolos de gestión de datos y carencias en la concienciación del personal sobre prácticas seguras. Además, se constató que las medidas de protección existentes eran insuficientes para salvaguardar la integridad, confidencialidad y disponibilidad de los datos utilizados en los procesos de mediación.

Por ejemplo: Se descubrió que la falta de cifrado en la comunicación digital y la ausencia de políticas claras de gestión de contraseñas eran áreas críticas que requerían atención inmediata.

4.2. DISEÑO DE MEJORA

El diseño de mejora implica proponer y planificar las acciones concretas que se llevarán a cabo para fortalecer la seguridad de datos en el centro de mediación

utilizando soluciones BAAS (Backup as a Service) y DRAAS (Disaster Recovery as a Service).

A continuación, se presenta una propuestas y planes de acción para mejorar la seguridad de datos en el centro de mediación:

4.2.1. Mejora de Infraestuctura de la Red de datos

Mejorar una infraestructura de red LAN básica como la que cuenta el centro de mediación, implica optimizar su rendimiento, seguridad y confiabilidad.

Hay que recordar que cada red es única y las mejoras deben adaptarse a las necesidades y recursos disponibles en cada caso, que permita que se puedan efectivamente realizar las mejoras necesarias en dicha estructura.

A continuación, se detallan algunas recomendaciones con ejemplos prácticos, para la red analizada:

1. Actualización de equipos y tecnologías: Reemplazar o actualizar los dispositivos de red antiguos por equipos más modernos y eficientes puede mejorar significativamente el rendimiento de la red. Por ejemplo, al momento se tienen switches de 100 Mbps, considerar la actualización a switches Gigabit Ethernet para aumentar la velocidad de transferencia de datos.

2. Optimización de cables y conexiones: Asegurarse de que los cables estén en buen estado, correctamente terminados y sin interferencias puede mejorar la estabilidad y la velocidad de la red. Además, en el presente caso se recomienda utilizar conexiones Ethernet en lugar de Wi-Fi cuando sea posible para reducir la congestión y mejorar la latencia.
3. Actualizaciones y parches: Mantener el firmware y el software de los dispositivos de red actualizado con las últimas versiones y parches de seguridad es fundamental para prevenir vulnerabilidades, así como, aplicaciones con licencia.

Es importante planificar cuidadosamente las actualizaciones y mejoras para minimizar el impacto en la operatividad de la red y garantizar un proceso fluido de implementación.

4.2.2. Investigación y selección de proveedores de servicios BAAS y DRASS que cumplan con los requisitos de seguridad y necesidades del centro.

Investigar y comparar diferentes proveedores de servicios de DRaaS y BaaS.

Evaluar la reputación, la experiencia y las características de cada proveedor.

Considerar la capacidad de recuperación, la seguridad y el soporte técnico ofrecidos por cada proveedor.

Ejemplo: Al comparar proveedores, se encuentra que Proveedor que ofrece una solución de DRaaS con replicación en tiempo real y recuperación instantánea, mientras

que Proveedor B ofrece un servicio de BaaS con almacenamiento en la nube y copias de seguridad programadas.

A continuación, se presenta información sobre los tres principales proveedores de DRaaS y BaaS del mercado, junto con algunos factores clave a considerar al seleccionar un proveedor:

Proveedor A: Amazon Web Services (AWS)

Características principales:

AWS ofrece una amplia gama de servicios en la nube, incluyendo opciones de DRaaS y BaaS.

Cuenta con una infraestructura global y altamente escalable.

Proporciona opciones flexibles de almacenamiento y recuperación de datos.

Ofrece herramientas de gestión y monitoreo avanzadas.

Factores a considerar:

Experiencia en la industria y una sólida reputación como proveedor de servicios en la nube.

Diversidad de servicios y opciones de personalización.

Escalabilidad y capacidad para satisfacer las necesidades futuras de crecimiento de la empresa.

Costo total de propiedad, considerando tanto el precio del servicio como los posibles costos adicionales.

Proveedor B: Microsoft Azure

Características principales:

Azure es una plataforma de servicios en la nube integral que incluye opciones de DRaaS y BaaS.

Ofrece una amplia gama de servicios y herramientas para respaldo, recuperación y seguridad de datos.

Integración con otras herramientas y servicios de Microsoft, como Office 365 y Active Directory.

Soporte para aplicaciones empresariales y entornos híbridos.

Factores a considerar:

- Ecosistema de Microsoft y capacidad de integración con otras soluciones y servicios existentes.
- Servicios y herramientas específicas para el respaldo y recuperación de datos.
- Cumplimiento normativo y seguridad de datos:

  Autenticación Multifactor (MFA):

  Azure Active Directory (Azure AD): Azure AD, parte integral de Azure, ofrece opciones de autenticación multifactor para proteger el acceso a los recursos en la nube. Los usuarios pueden habilitar MFA para agregar una capa adicional de seguridad.

  Revisión Regular de Permisos:

Azure RBAC (Role-Based Access Control): Permite asignar roles específicos a los usuarios y revisar periódicamente los permisos asignados. Los administradores pueden auditar y ajustar los roles para asegurar que los usuarios tengan los privilegios necesarios.

Restricciones de Acceso Basadas en Roles:

Azure RBAC: Permite definir roles personalizados y asignarlos a usuarios o grupos. Esto asegura que cada usuario tenga acceso solo a los recursos necesarios para sus responsabilidades.

Registro de Acceso:

Azure Monitor y Azure Security Center: Proporcionan capacidades de registro y monitorización avanzadas. Azure Monitor puede rastrear actividades en la plataforma, y Azure Security Center ofrece una vista integral de la seguridad con registro de actividades y alertas.

Protección de Cuentas Privilegiadas:

Azure AD Privileged Identity Management (PIM): Permite administrar, controlar y supervisar el acceso a recursos de Azure, incluyendo funciones de administrador. PIM ayuda a proteger cuentas privilegiadas.

- Soporte técnico y recursos de la comunidad.

Proveedor C: Google Cloud Platform (GCP)

Características principales:

GCP ofrece una amplia gama de servicios en la nube, incluyendo opciones de DRaaS y BaaS.

Escalabilidad y rendimiento de clase empresarial.

Herramientas de gestión y monitoreo avanzadas.

Enfoque en la innovación y el desarrollo de soluciones basadas en inteligencia artificial y aprendizaje automático.

Factores a considerar:

Capacidades de análisis y procesamiento de datos avanzadas.

Precios competitivos y opciones de facturación flexibles.

Capacidad para trabajar con otras soluciones y servicios de Google.

Soporte técnico y recursos de la comunidad.

Es importante tener en cuenta que la elección del proveedor adecuado dependerá de las necesidades y requisitos específicos de cada centro de mediación, así como de consideraciones tales como: costos, la integración con sistemas existentes, la experiencia y la capacidad de soporte técnico.

En este caso se opta por la Opción del Proveedor B, considerando las bondades de la plataforma y la familiaridad del personal que labora en la entidad con el entorno de Microsoft, adicionalmente por limitaciones de costo se recomienda empezar utilizando la plataforma básica de Microsoft, para luego escalar a los servicios de Azure.

Costos de Implementación:

De la investigación realizada se obtienen los siguientes valores a la fecha en que se realiza el presente estudio:

Tabla 4

Análisis de costos de implementación

Inversión	Descripción	Caso de estudio
Costo de Adquisición de Soluciones	Costo de adquirir las soluciones BAAS y DRAAS, incluyendo licencias, hardware y/o servicios de terceros.	El costo total de adquirir las soluciones BAAS y DRAAS está alrededor de $14,000 que incluye las licencias y servicios de respaldo.
Costo de Instalación y Configuración	Costo de la instalación y configuración de las soluciones en la infraestructura del centro de mediación.	El costo de instalación y configuración de las soluciones BAAS y DRAAS es de $2,000.

Fuente: Elaboración Propia

Vale la pena indicar que se puede iniciar con soluciones básicas, económicas y luego ir escalando conforme crece la necesidad de la entidad.

Beneficios Esperados

Tabla 5

Análisis de beneficios de la implementación

Actividad	Descripción	Beneficio
Mejora en la Seguridad de Datos	Reducción del riesgo de pérdida de datos y aumento en la protección de la información confidencial de importancia para el centro de mediación, como para los usuarios del servicio.	La implementación de BAAS y DRAAS permite al centro de mediación recuperar rápidamente sus datos en caso de un desastre y asegurar la confidencialidad de la información de los clientes.
Reducción del Tiempo de Recuperación	Disminución del tiempo de inactividad en caso de una interrupción o desastre, lo que aumenta la disponibilidad del servicio.	El tiempo de recuperación de datos en caso de un desastre se reduce de 48 horas a 4 horas gracias a las soluciones DRAAS.
Cumplimiento de Normativas	Cumplimiento de regulaciones y normativas de protección de datos, evitando sanciones legales.	La implementación de soluciones BAAS y DRAAS asegura el cumplimiento de

		regulaciones de protección de datos vigentes en el país.

Fuente: Elaboración Propia

Si se considera que la pérdida de una Acta de mediación por ejemplo, puede causar graves dificultades al centro de mediación, porque dichos documentos deben ser reportados al Concejo de la Judicatura para que sea de cumplimiento obligatorio de las partes, pues, de no registrarse dicho documento, puede causar sanciones al centro de mediación, así como, daños personales y materiales de incalculable valor a los ususarios del servicio, ya que una mediación puede ser desde tipo familiar donde está en riesgo la integridad de las personas que es algo invaluable hasta por ejemplo la mediación de una repartición de herencias donde hay un costo material que bien puede superar de largo la inversión que se realice en proteger la información, ya que dichos documentos tienen fuerza de sentencia que debe cumplirse a satisfacción de las partes.

4.2.3. Instalación y Configuración del software BASS Y DRAAS para establecer un plan de recuperación ante diferentes tipos de desastres (por ejemplo, incendios, fallas de hardware, etc.).

Debido a las limitaciones económicas del momento, no se pudo adquirir el software principal Azure seleccionado anteriormente, sin embargo, en el momento que se

dispongan los recursos se deberá aplicar lo siguiente: Instalar y Configurar el entorno de recuperación en la nube del proveedor seleccionado.

Establecer la replica de datos desde los sistemas locales a la infraestructura en la nube.

Realizar pruebas de recuperación para garantizar la disponibilidad y la integridad de los datos.

En este caso se deberá configurar la infraestructura de recuperación en la nube del Proveedor B y se establecerá la replica de los archivos de diseño desde la Red local a la nube. Se realizarán pruebas periódicas para verificar que los archivos se puedan recuperar adecuadamente en caso de un desastre.

Los archivos de clientes y la base de datos se replicarán automáticamente cada 15 minutos hacia el entorno de recuperación en la nube.

Es importante seguir las recomendaciones y las guías proporcionadas por el proveedor seleccionado, así como adaptar los pasos según sea necesario para cumplir con los requisitos y objetivos de protección y recuperación de la entidad estudiada.

4.2.4.Pruebas de Recuperación

Se deberán realizar pruebas regulares de recuperación para asegurarse de que los datos se puedan restaurar correctamente en caso de un desastre. Evaluar y

documentar los resultados de las pruebas, identificando áreas de mejora si es necesario.

Por ejemplo, se pueden realizan pruebas de recuperación simulando diferentes escenarios de desastre, como una pérdida total de los sistemas locales. Se verificará que los archivos de clientes y la base de datos se puedan restaurar adecuadamente desde el entorno de recuperación en la nube.

4.2.5. Creación de políticas de seguridad de la entidad para incluir directrices específicas sobre el uso de BaaS y DRaaS, asi como de uso de claves de usuario en base a perfiles.

Se deberá determinar la frecuencia y el horario de los respaldos según los requisitos de la empresa.

Establecer la retención de los respaldos, es decir, cuánto tiempo se deben conservar los datos respaldados.

Definir niveles de acceso para cada usuario y definir claves de acceso, inicialmente y a futuro, realizar una serie de acciones como:

Revisión Regular de Permisos

Restricciones de Acceso Basadas en Roles

Registro de Acceso.

Protección de Cuentas Privilegiadas, etc.

En el presente caso, se establece que los respaldos de los archivos de clientes se deben realizar diariamente al final del día laboral y se conservarán durante un período de 60 días.

Se debe configurar los sistemas locales para realizar respaldos automáticos de los datos identificados como críticos.

Verificar que los respaldos se estén realizando correctamente y que los datos estén siendo transferidos al entorno de respaldo en la nube.

Se debe configurar el software de respaldo en los servidores de la empresa para realizar respaldos automáticos de las bases de datos y los archivos de clientes. Se verificará que los respaldos se realicen de manera exitosa y que los datos sean transferidos al entorno de respaldo en la nube del proveedor B.

4.2.6. Concienciación del personal:

La concienciación del personal es fundamental para crear una cultura de seguridad en la organización. Esto implica capacitar y educar a los empleados sobre buenas prácticas de seguridad, cómo reconocer amenazas potenciales como el phishing y cómo proteger los datos confidenciales.

La concienciación del personal es una línea de defensa importante para prevenir ataques cibernéticos.

4.3. Mecanismos de Control

Monitoreo y mantenimiento

Se deberá realizar un monitoreo continuo de los sistemas de DRaaS y BaaS para garantizar su funcionamiento adecuado.

Actualizar y probar regularmente los planes de recuperación y las políticas de copia de seguridad.

Mantener una comunicación constante con el proveedor de servicios para resolver problemas y recibir soporte técnico.

En el presente caso se establece un proceso de monitoreo para verificar que la replica de datos del Proveedor B y las copias de seguridad se realicen correctamente.

Se actualizarán los planes de recuperación y las políticas de copia de seguridad cada seis meses y se realizará un seguimiento regular con los proveedores para resolver cualquier problema.

A continuación, se presenta un desglose punto por punto del proceso de: Monitoreo y mantenimiento a seguir en la implementación de DRaaS y BaaS:

- Establecer un programa de monitoreo:

Configurar herramientas de monitoreo para supervisar el entorno de DRaaS y BaaS de manera continua.

Establecer alertas y notificaciones para detectar posibles problemas o eventos no deseados, así como la integridad de los datos respaldados.

Configurar alertas para recibir notificaciones en caso de interrupciones o fallas.

- Realizar revisiones periódicas:

Realizar revisiones regulares del entorno de DRaaS y BaaS para asegurarse de que esté funcionando de manera óptima.

Evaluar el rendimiento y la eficacia de los servicios de DRaaS y BaaS y tomar medidas correctivas si es necesario.

En el presente caso se recomienda realizar revisiones mensuales del entorno de DRaaS y BaaS para verificar que los respaldos se estén realizando correctamente, que los tiempos de recuperación sean adecuados y que los objetivos de nivel de servicio se cumplan.

- Mantener actualizaciones y parches:

Mantener actualizados los componentes del entorno de DRaaS y BaaS, como el software y los sistemas operativos, aplicando los parches y actualizaciones de seguridad correspondientes.

- Realizar pruebas de recuperación:

Es importante realizar pruebas periódicas de recuperación para verificar la capacidad de restauración de los datos y aplicaciones respaldados.

Evaluar los resultados de las pruebas y realizar ajustes si es necesario.

En el centro de mediación se pueden realizar pruebas trimestrales de recuperación para simular diferentes escenarios de desastre y verificar que los datos y aplicaciones respaldados se puedan restaurar adecuadamente.

- Gestionar incidentes y problemas:

Establecer un proceso de gestión de incidentes y problemas para abordar y resolver de manera eficiente cualquier incidente o problema relacionado con el entorno de DRaaS y BaaS.

En este tema es aconsejable mantener un registro de incidentes y problemas, asignar responsabilidades para su resolución y realizar análisis de causa raíz para prevenir recurrencias.

Capacitación y actualización del personal:

Proporcionar capacitación regular al personal encargado de la supervisión y mantenimiento del entorno de DRaaS y BaaS.

Mantener al personal actualizado sobre las mejores prácticas de seguridad y las novedades en el ámbito de la protección de datos.

- Mantenimiento y monitoreo continuo

Realizar un monitoreo continuo del entorno de recuperación para asegurarse de que esté funcionando correctamente.

Mantener actualizados los planes de recuperación y las políticas de replicación de datos según las necesidades cambiantes de la oficina.

Comunicarse regularmente con el proveedor de DRaaS para resolver problemas y recibir soporte técnico.

CAPITULO V: SUGERENCIAS

5.1 Recomendaciones

En base al trabajo realizado, es importante realizar las siguientes sugerencias:

- Una recomendación clave es establecer una Política de Seguridad de la Información que contemple la protección y el manejo adecuado de los datos en los centros de mediación. Esta política debe incluir directrices claras sobre el uso de contraseñas seguras, acceso a la información, respaldo de datos, manejo de dispositivos móviles y la realización periódica de auditorías de seguridad. Se debe capacitar a todo el personal involucrado en la mediación en línea para que comprenda y aplique adecuadamente las políticas de seguridad.

  En el caso práctico: El centro de mediación puede implementar una política que establezca que todas las cuentas de usuario deben tener contraseñas robustas y se deben cambiar regularmente. Además, se puede requerir que los dispositivos utilizados para acceder a la información estén protegidos con contraseñas o reconocimiento biométrico. También se podría establecer una política de respaldo diario de la información en la nube y almacenar copias de seguridad fuera del sitio para garantizar la disponibilidad en caso de desastre.

  2: Capacitar al Personal y las Partes Involucradas: Es esencial brindar capacitación continua al personal y a las partes involucradas en la mediación en línea sobre las mejores prácticas de seguridad de la información. Esto incluye

educar sobre la detección de phishing, la protección contra malware y el manejo seguro de datos confidenciales. La concienciación sobre seguridad debe ser un proceso constante y actualizado a medida que surjan nuevas amenazas.

Para el centro de mediación: Se pueden organizar sesiones de capacitación periódicas en seguridad de la información para el personal y los mediadores que operan en el centro. Además, se podría proporcionar a los usuarios una guía de buenas prácticas en seguridad que incluya recomendaciones para evitar el acceso no autorizado a sus cuentas y cómo identificar correos electrónicos o enlaces sospechosos.

3: Establecer un Equipo de Respuesta a Incidentes: El centro de mediación debe contar con un equipo de respuesta a incidentes que pueda actuar rápidamente en caso de que se produzca un evento de seguridad. Este equipo debe estar preparado para identificar, mitigar y resolver cualquier incidente que afecte la seguridad de la información, minimizando el impacto y asegurando una pronta recuperación.

En nuestro caso: El equipo de respuesta a incidentes podría estar compuesto por personal técnico capacitado en ciberseguridad, representantes legales y representantes de la alta dirección del centro de mediación. Si se detecta un intento de acceso no autorizado a la plataforma de mediación, este equipo

actuaría de inmediato para bloquear el acceso, investigar la causa y tomar medidas para prevenir futuros intentos.

4: Monitorear y Evaluar Constantemente la Seguridad: La seguridad de la información es un proceso en constante evolución, por lo que es importante realizar un monitoreo y evaluación continuos de los sistemas de seguridad implementados. Se deben revisar periódicamente las políticas y medidas de seguridad, realizar pruebas de vulnerabilidad y realizar auditorías para garantizar el cumplimiento de los estándares y regulaciones establecidas.

5: Cronograma

A continuación, se presenta un ejemplo de un cronograma para diseñar un plan de implementación de normas de seguridad informática en los centros de mediación Online Dispute Resolution (ODR). Este cronograma es solo una referencia y puede variar según las necesidades y características específicas de cada centro de mediación ODR.

Actividades	**Duración estimada**
- Realizar un diagnóstico de seguridad actual	1 Semanas
- Investigar proveedores BASS y DRAAS	1 Semana
- Diseñar un plan de Implementación	2 Semanas
- Adquirir e Instalar soluciones	1 Semana
- Capacitar al personal en nuevas soluciones	2 Semanas

- Realizar pruebas de seguridad	1 Semanas
- Implementar medidas de seguridad	2 Semanas
- Establecer mecanismos de control	1 semana
- Monitorear y actualizar seguridad	Continuo

Fuente: Elaboración Propia

Es importante destacar que este cronograma es solo una guía general y que el tiempo requerido para cada etapa puede variar según la complejidad y el tamaño del centro de mediación ODR, así como los recursos disponibles. Además, es fundamental adaptar el plan de implementación de seguridad informática a las necesidades y particularidades específicas de cada centro de mediación ODR, y asegurarse de cumplir con las normas y regulaciones pertinentes en materia de seguridad de la información.

Para el caso de estudio: Se puede establecer un programa de monitoreo y evaluación trimestral que incluya pruebas de penetración, revisión de logs de seguridad y análisis de incidentes pasados. Además, se podría realizar una auditoría externa para evaluar la conformidad con estándares de seguridad reconocidos, como ISO 27001.

En conjunto, estas recomendaciones permitirán al centro de mediación fortalecer su seguridad de la información digital y garantizar un entorno seguro y confiable para todas las partes involucradas en el proceso de mediación en línea. Al adoptar una enfoque proactivo y comprometido con la seguridad, el centro de mediación podrá

proteger los datos de manera efectiva y mantener la confianza de sus usuarios en la integridad del proceso de mediación.

5.2 Conclusiones

En base a los objetivos planteados podemos ver que la propuesta de implementación de las seguridades BAAS (Backup as a Service) y DRaaS (Disaster Recovery as a Service), es de mucha importancia para los centros de mediación, así como para la calidad de servicio y satisfacción del cliente, lo que nos permite concluir que:

- Con la implementación de las soluciones BAAS y DRaaS, se tendrá un avance significativo en la seguridad de la información digital de los centros de mediación en línea en Quito. Estas soluciones brindarán respaldo y recuperación ante desastres, lo que garantiza la integridad, confidencialidad y disponibilidad de los datos en situaciones adversas. Asimismo, permiten el cumplimiento de los objetivos específicos planteados.
- El estudio para la implementación de BAAS y DRaaS permitieron realizar un diagnóstico exhaustivo de la situación actual de los sistemas de seguridad en el centro de mediación. Se identificaron las fortalezas y debilidades en materia de infraestuctura y seguridad de la información, lo que proporcionó una base sólida para el diseño de estrategias y mejoras efectivas.
- Gracias a las funcionalidades de BAAS y DRaaS, fue posible identificar las vulnerabilidades y riesgos asociados a la seguridad de la información. Se detectaron posibles amenazas que podrían afectar la integridad de los datos,

como ataques cibernéticos, errores humanos o fallos técnicos. Esto permitió tomar medidas proactivas para mitigar dichos riesgos y garantizar la protección de la información de manera efectiva.

- La implementación de BAAS y DRaaS permitirá diseñar medidas y prácticas de seguridad específicas para fortalecer la protección de la información digital en los centros de mediación. Se pueden establecer copias de respaldo automáticas y un plan de recuperación ante desastres, lo que asegura la disponibilidad de la información en caso de incidentes. Además, se pueden implementar controles para el acceso y uso adecuado de los datos, lo que reduce significativamente las posibilidades de violaciones de seguridad.
- Para la implementación de BAAS y DRaaS, se determinan mecanismos de control para evaluar la efectividad de las mejoras en seguridad a implementarse. Estos mecanismos incluyen pruebas de restauración y simulacros de recuperación ante desastres, lo que permite verificar la correcta configuración y funcionamiento de las soluciones.

En resumen, la implementación de las soluciones BAAS y DRaaS traen como resultado, un aumento significativo en la seguridad de la información digital de los centros de mediación en línea en Quito y puede extenderse a nivel nacional sin mayores inconvenientes. Estas soluciones proporcionan una protección robusta y una rápida recuperación ante desastres, garantizando la continuidad de las operaciones y la confianza de los usuarios, adicionalmente, se puede iniciar con aplicaciones básicas y luego escalar a plataformas más robustas y especializadas.

El diagnóstico, identificación de vulnerabilidades, diseño de medidas de seguridad y recomendación de mecanismos de control son fundamentales para lograr avances, asegurando un entorno seguro y confiable para la resolución de disputas en línea.

BIBLIOGRAFIA

Álvarez, JMD y Lezama, JC (2016). Buenas prácticas en seguridad informática para usuarios finales en empresas. Revista Visión de Futuro, 20 (2), 5-24.

Alarcón, F., Muñoz, C., & Cifuentes, D. (2016). Buenas prácticas para la seguridad de la información en las organizaciones. Revista INNOVA Revista de Investigación, 1 (4), 44-53.

Ciampa, M. (2020). Seguridad+ Guía de estudio del examen SY0-501 (7.a ed.) . Aprendizaje Cengage.

García, MJM y Escalante, HJM (2012). *Seguridad informática: Cómo proteger los sistemas de informaciónSeguridad informática: Cómo proteger los sistemas de información en la empresa (3.a ed.) . Ra-Ma.

García, MJM y Escalante, HJM (2012). Seguridad informática: Cómo proteger los sistemas de información en la empresa (3.a ed.) . Ra-Ma.

Organización Internacional de Normalización. (2013). ISO/IEC 27001:2013 Sistemas de gestión de seguridad de la información - Requisitos (1.a ed.) . YO ASI.

Obispo, M. (2018). Seguridad informática: Principios y prácticas (3.a ed.) . Pearson.

NIST. (2018). Framework para mejorar la ciberseguridad de la infraestructura crítica (Versión 1.1) . Autor.

Pérez, DA y Villalba, JLR (2019). Buenas prácticas de seguridad informática en la empresa: Análisis de los factores críticos de éxito. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (33) , 16-26.

Pfleeger, CP y Pfleeger, SL (2014). Seguridad de sistemas informáticos: Conceptos y aplicaciones (5.a ed.) . Prentice Hall.

Schneier, B. (2015). *Secretos y mentiras: La seguridad en la era de la información (20.a ed.) . Wiley.

Sitio web de ODR Ecuador. (sf). https://odrecuador.com

Stoll, C. (2012). El diario del intruso: La verdadera historia de un hacker llamado Stoll (3.a ed.) . Medios O'Reilly.

Ubierna, S.A.Guía ISO 27001: Implantación práctica (1.a ed.) . ENI Ediciones.

Vidal, ER y Granda, FJ (2018). Propuesta de buenas prácticas para la seguridad de la información en la empresa. Revista Espacios, 39 (42), 1-14.

Whitman, ME y Mattord, HJ (Principios de seguridad de la información y gestión (3.a ed.) . Aprendizaje Cengage.

ANEXOS

DOCUMENTACION DEL PROCESO

Tabla 1: *Evaluación de la Infraestructura de Seguridad*

Aspecto a Evaluar	Descripción	Resultado
Infraestructura de Red		
Firewall		
Acceso Remoto		
Seguridad de Servidores		

Fuente: Elaboración Propia

Tabla 2: *Tabla de evaluación de datos y aplicaciones críticas:*

Recurso	**Importancia para el negocio**	**Nivel de protección requerido**	**Nivel de recuperación requerido**
Base de datos de clientes			
Aplicación de contabilidad			
Actas de mediación y sus soportes.			
Videos de las sesiones de mediación			
Informes de Actas emitidos a la Judicatura			

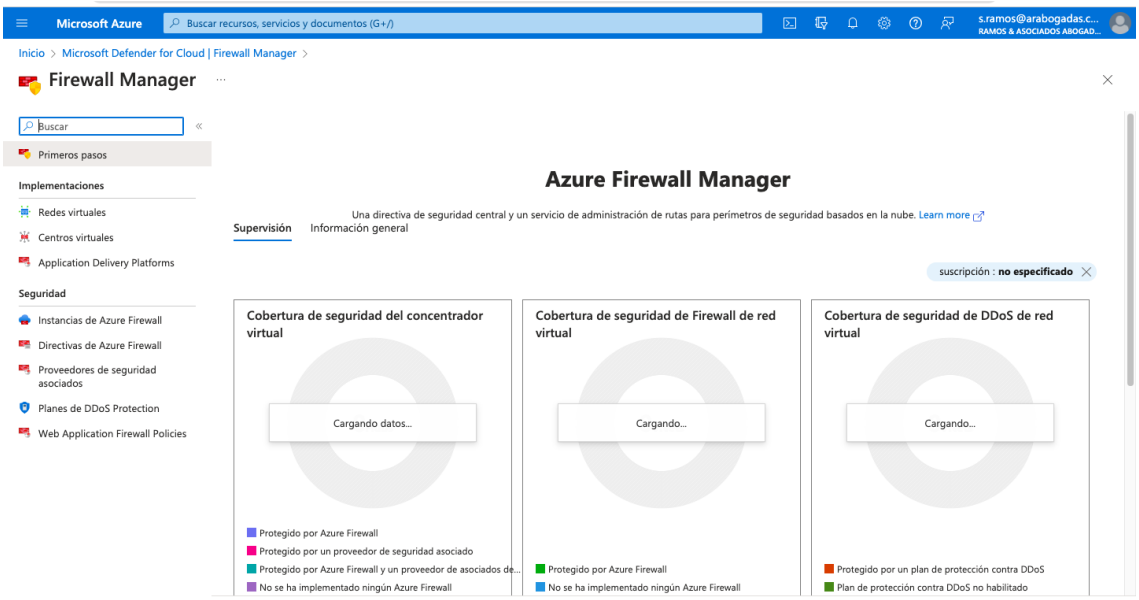
Fuente: Elaboración Propia

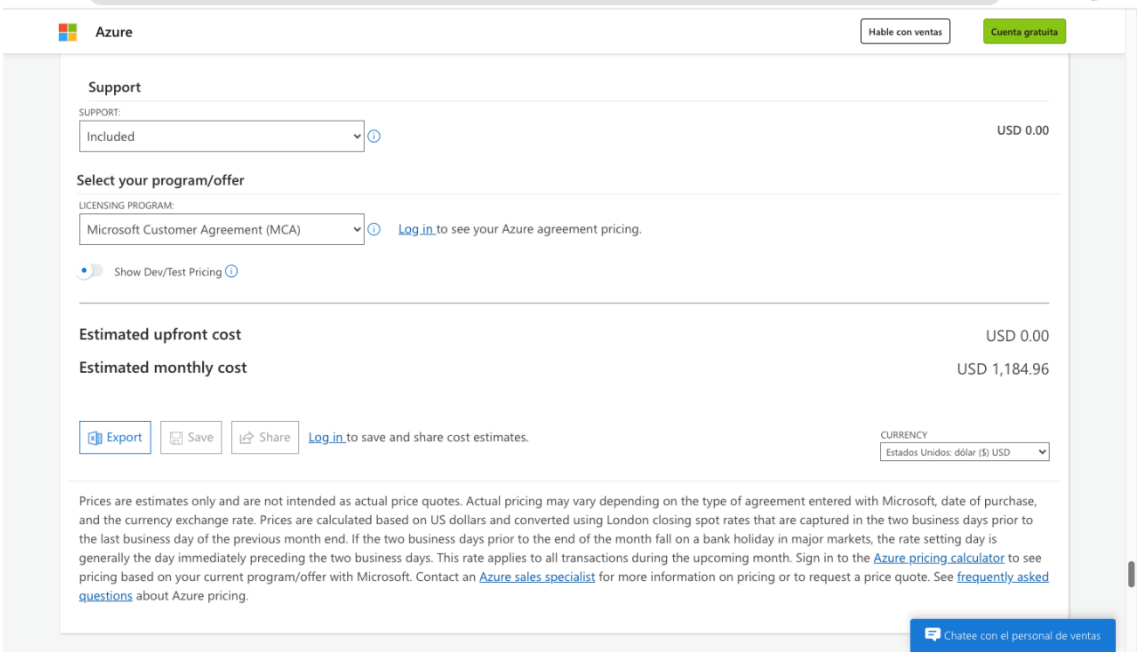
Tabla 3: *Formulario de requisitos de protección y recuperación:*

	Archivo1	**Archivo2**	**Archivo3**	**Archivo4**
Recurso:				
Importancia para el negocio:				
Requisitos de protección:				
Frecuencia de respaldo:				
Retención de respaldo:				
Ubicación del respaldo:				
Método de cifrado:				
Requisitos de recuperación				
RTO (Objetive Recovery Time)				
RPO (Objetive Recovery Point)				
Proceso de Recuperación				

Fuente: Elaboración Propia

PRESUPUESTO SERVICOS





Nota: Detalle de presupuesto de plataforma Azure. Fuente: Página web oficial de Azure.

Recuperado el [08-2023] de https://portal.azure.com/#allservices/category/Storage