UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS
ESCUELA DE INGENIERÍA INFORMÁTICA

Propuesta de una metodología para el gestionamiento de la documentación en la nube para la empresa Golden Comunicaciones S. A.

MODALIDAD PROYECTO PARA OPTAR POR EL GRADO DE BACHILLER EN INGENIERÍA DE (INFORMÁTICA, SISTEMAS, SOFTWARE)

María Camila Figueroa Mora

San José, Costa Rica

Enero de 2025

DEDICATORIA

Dedico este trabajo, en primer lugar, a Dios, por iluminar mi camino, darme la fortaleza para superar cada desafío y permitirme alcanzar una de las metas más importantes de mi formación profesional.

A mi familia, por ser mi mayor inspiración, por su amor, paciencia, sacrificio y apoyo incondicional en cada etapa de mi vida. Gracias por creer en mí y motivarme a seguir adelante aun en los momentos más difíciles.

A mis amistades y a todas las personas que me brindaron palabras de aliento, comprensión y acompañamiento durante este proceso, mi más profundo agradecimiento.

Finalmente, me dedico este logro a mí misma, por la constancia, el esfuerzo, la disciplina y la perseverancia demostradas para convertir este sueño en una realidad. Que este sea el inicio de nuevos retos y oportunidades de crecimiento tanto personal como profesional.

María Camila Figueroa Mora

AGRADECIMIENTOS

En primer lugar, agradezco a Dios por brindarme la fortaleza, la salud y la sabiduría necesarias para culminar esta importante etapa de mi vida académica.

Expreso mi más sincero agradecimiento a mi familia por su amor incondicional, apoyo constante, comprensión y motivación durante todo este proceso. Su confianza en mí ha sido un pilar fundamental para alcanzar esta meta.

A mi persona tutora y al comité asesor, les agradezco por su orientación, conocimientos, tiempo y valiosas observaciones, las cuales contribuyeron significativamente al desarrollo y fortalecimiento de esta investigación.

Asimismo, extiendo mi agradecimiento a la empresa **Golden Comunicaciones S.A.**, por permitirme desarrollar este proyecto y facilitar la información necesaria para la realización del estudio. De igual forma, agradezco a todas las personas colaboradoras que brindaron su apoyo y disposición durante el proceso de investigación.

Finalmente, agradezco a todas aquellas personas que, de una u otra manera, contribuyeron al logro de este objetivo y me acompañaron durante este camino académico. Este trabajo representa el resultado del esfuerzo, la perseverancia y el apoyo recibido de cada una de ellas.

María Camila Figueroa Mora

CONTENIDO

TABLAS

FIGURAS

ANEXOS

CAPÍTULO I: INTRODUCCIÓN

Descripción del Problema

Golden Comunicaciones es una empresa con más de trece años de trayectoria dedicada al desarrollo y arrendamiento de infraestructura para el sector de las telecomunicaciones. Su labor contribuye al crecimiento de los operadores de telecomunicaciones mediante la ampliación de las redes y de esta manera brindar mejores servicios a la población.

La empresa ofrece soluciones de infraestructura para el despliegue de las telecomunicaciones. Asimismo, implementa un sistema de gestión integral que abarca la calidad, el medio ambiente, la seguridad y la salud en el trabajo, el cual responde a las expectativas de su equipo de trabajo y satisface los requisitos de sus clientes.

En relación con dicho sistema de gestión integral, la empresa asigna los recursos necesarios para su implementación y para asegurar el cumplimiento de las normas ISO 9001, ISO 14001 y OHSAS 18001, promoviendo la mejora continua de sus procesos y procedimientos.

A través de un estudio se identificaron diversos problemas que actualmente afectan la productividad administrativa de ella. Estas dificultades se originan debido a que su información se almacena en un servidor NAS ubicado en otro país, lo que dificulta el acceso oportuno para atender incidentes, solucionar problemas técnicos y administrar adecuadamente la información.

Los principales problemas identificados son los siguientes:

a) Errores de bloqueo en archivos y carpetas.
b) Alteración de permisos a los usuarios externos.
c) Perdida de información.
d) Bajo rendimiento laboral y producción administrativamente en los colaboradores.

El servidor almacena más de 1000 archivos, entre carpeta, fotografías y archivos de la aplicación de Microsoft Excel, PowerPoint y Word, Con el pasar del tiempo, a pesar de contar con una amplia capacidad de almacenamiento, su velocidad y acceso a los archivos se ha vuelto de manera más lenta, haciendo que el acceso de los usuarios sea muy vulnerable y de manera peligrosa. Además, en múltiples ocasiones se han eliminado o piérido archivos por conflicto entre usuarios, lo que genera fallas de sincronización y desconexiones inesperadas del sistema.

La conexión al servidor se realiza de forma remota mediante la búsqueda de una IP local y se activa en ubicaciones locales de red del equipo, lo que incrementa la dependencia de estabilidad de la red y de configuraciones técnicas específicas.

Adicionalmente, para establecer la conexión remota al servidor es necesaria la descarga e instalación de una aplicación red privada virtual (VPN), mediante la cual el usuario debe autenticarse utilizando un nombre de red, el nombre del usuario y la contraseña. Aunque este procedimiento incorpora un nivel adicional de seguridad, también incrementa la complejidad operativa y la probabilidad de errores de conexión. Asimismo, cuando ocurre una interrupción en la desconexión de red donde se encuentra alojado el servidor, se pierden todos los accesos a las carpetas o archivos. Todo esto impacta directamente en el bajo rendimiento laboral y en la disminución de la productividad administrativa, ya que los colaboradores deben invertir tiempo adicional en recuperar documentos, rehacer trabajos o esperar el restablecimiento del acceso.

Otro problema consiste en que la empresa cuenta con usuarios que no permanecen físicamente en una ubicación administrativa fija, lo que implica que dependen de conexiones externas y redes con condiciones variables para acceder a la información. Si no disponen de una conexión previamente configurada o suficientemente estable, no pueden ingresar al sistema, lo que limita la flexibilidad operativa y dificulta el desarrollo del trabajo remoto o en campo.

Esta situación evidencia la necesidad de una solución tecnológica más escalable, segura y accesible desde diferentes ubicaciones, sin comprometer la integridad ni la disponibilidad de la información corporativa.

En conjunto, estos factores reflejan debilidades estructurales en el modelo actual de gestión documental y almacenamiento, lo que hace indispensable la implementación de una metodología más eficiente, segura y alineada con buenas prácticas internacionales en gestión de la información.

Objetivos

Objetivo General

Elaborar una propuesta de metodología para el gestiona miento de la documentación en la nube basada en Microsoft OneDrive, para la empresa Golden Comunicaciones S.A., apoyada en lineamientos de buenas prácticas internacionales como ISO 27001, ISO 9001 e ITIL, con el fin de mejorar la seguridad, control, acceso y administración de la información corporativa.

Objetivos Específicos

a) Crear controles de bloqueo que prevengan errores en archivos y carpetas.
b) Elaborar procedimientos que controlen los daños generados por los usuarios.
c) Elaborar controles de seguridad para la reducción de errores que se tienen por parte de los usuarios en el acceso a las carpetas.
d) Diseñar un plan de recuperación que permita el control de versiones en todos los documentos y archivos de la organización, garantizando que cada cambio quede registrado y se pueda acceder a versiones anteriores en caso de pérdida o modificación no deseada.

Justificación

La investigación se lleva a cabo con el propósito de diseñar una metodología estructurada para el manejo de la documentación de la nube, específicamente en Microsoft OneDrive, que permita a la empresa Golden Comunicaciones S.A. mejorar la seguridad, el control, el acceso y la administración de su información corporativa.

¿Qué beneficios pueden reportar los resultados obtenidos?

a) **Mayor seguridad de la información:** Al establecer controles de acceso, bloqueo y protección de documentos.
b) **Reducción de errores humanos:** Mediante procedimientos claros y controles definidos para el uso de archivos y carpetas.
c) **Mejor control y trazabilidad de la documentación:** Gracias a la implementación de versiones y registros de cambios.
d) **Mejora en la continuidad operativa:** Al contar con planes de recuperación ante pérdidas o modificaciones no deseadas de documentos.

Viabilidad

Viabilidad Técnica

La investigación es técnicamente viable debido a que la empresa Golden Comunicaciones S.A. cuenta con la infraestructura tecnológica necesaria para el desarrollo e implementación de una metodología de gestión documental en la nube basada en Microsoft OneDrive. Esto significa que no requiere el desarrollo de un software desde cero, sino de la configuración y estructuración de las herramientas tecnológicas adecuadas.

La condición que hace posible el desarrollo del prototipo es que la organización ya cuenta con una infraestructura tecnológica operativa, acceso a internet estable y licencias de Microsoft 365. Esto permite utilizar funcionalidades como control de versiones, gestión de permisos, auditoría de cambios y recuperación de archivos sin la necesidad de adquirir un sistema adicional.

Recursos tecnológicos para utilizar

Hardware

a) Existen doce equipos de cómputo (computadoras portátiles).
b) Dispositivos móviles con acceso corporativo al correo y Teams.
c) Infraestructura de red interna.

d) Conexión estable a internet y datos móviles en los celulares corporativos.

Software

a) Instalación de Microsoft OneDrive.
b) Suite de Microsoft 365 (SharePoint, Outlook, Teams).
c) Programas de Office (Excel, PowerPoint, Word).
d) Sistema operativo de Windows.
e) Navegadores web actualizados.

Licencias

a) Licencias corporativas activas de Microsoft 365
b) Cuentas institucionales para acceso controlado

Infraestructura y Espacio físico

a) No se requiere espacio adicional para servidores físico, ya que el almacenamiento se realiza en la nube.
b) Se utilizan oficinas y estaciones de trabajo ya disponibles en la empresa.

Para el desarrollo de la investigación, la plataforma a desarrollar que se utiliza tiene un costo específico y dispone de diferentes tipos y características. Se selecciona el Microsoft Office Empresarial. Si la empresa ya cuenta con una licencia, se puede optar por una expansión de memoria y almacenamiento para cada usuario; también se puede optar por una licencia adicional destinada únicamente al alojamiento de las carpetas y archivos.

Desde un punto de vista técnico, el proyecto es viable porque aprovecha recursos tecnológicos ya implementados en la organización y se apoya en una plataforma robusta, segura y escalable, garantizando que su implementación puede hacerse sin limitaciones técnicas.

Viabilidad Operativa

Es una metodología propuesta para la gestión de la documentación en la nube está diseñada para que sea de fácil uso y pueda ser adoptada e implementada por los usuarios. Microsoft OneDrive es una herramienta ya conocida y sencilla en el entorno laboral.

Los conocimientos requeridos para la implementación y el uso del sistema incluyen nociones básicas sobre las herramientas de Microsoft 365, específicamente OneDrive. Asimismo, es necesario comprender los procedimientos internos relacionados con la gestión documental y la seguridad de la información. En cuanto al personal calificado, la organización cuenta con colaboradores que poseen conocimientos básicos en el uso de herramientas tecnológicas, lo que

les permite adoptar adecuadamente la propuesta de solución. Además, se dispone de un departamento encargado del área de Tecnologías de la Información (TI), el cual brindará soporte técnico y realizará la supervisión del manejo y funcionamiento de la plataforma.

Por otra parte, se identifica la necesidad de una capacitación básica enfocada en la seguridad y el control adecuado para la manipulación de los documentos, carpetas y datos que serán almacenados en la nube. El prototipo será utilizado principalmente por el personal administrativo, operativo y técnico de la empresa, así como por los responsables de gestión documental y el área de TI. Adicionalmente, existirán usuarios responsables exclusivamente de la gestión documental, así como el área de TI, que llevará a cabo una revisión constante y proporcionará soporte continuo para garantizar el correcto funcionamiento del sistema.

Viabilidad Económica

La investigación no genera un impacto financiero para la empresa; por el contrario, contribuye a la reducción de costos.

A continuación, se resumen los costos estimados para la empresa:

Tabla 1

Centro de Costos

Concepto	Descripción	Costo estimado	Justificación
Licencias de software	Uso de Microsoft OneDrive incluido en Microsoft 365	₡0 / $0	La empresa ya cuenta con licencias activas; no se requiere inversión adicional.
Infraestructura tecnológica	Equipos de cómputo, red y almacenamiento en la nube	₡0 / $0	Se utiliza infraestructura existente y servicios en la nube.
Desarrollo de la investigación	Análisis, diseño de la metodología, elaboración de procedimientos y controles	₡0 / $0	Se realiza como parte de un proyecto académico, sin contratación externa.
Costos operativos y mantenimiento	Administración y monitoreo del sistema	₡0 / $0	Incluido dentro de las actividades normales del área de TI.

Licencias de software	Uso de Microsoft OneDrive incluido en Microsoft 365	₡0 / $0	La empresa ya cuenta con licencias activas; no se requiere inversión adicional.

Nota. Elaboración propia, 2026

Viabilidad legal

Se asume que la empresa Golden Comunicaciones S.A. cumple con la legislación nacional vigente en materia de protección de datos, confidencialidad de la información y uso de tecnologías. Asimismo, la organización dispone de políticas internas básicas que confirman el correcto manejo de información y uso de herramientas tecnológicas.

La investigación presenta como limitación el hecho de que no contempla la modificación de leyes, reglamentos o normativas externas; se enfoca principalmente en la adecuación de los procesos internos de la empresa. La propuesta se restringe al uso de plataformas tecnológicas previamente autorizadas por la organización, en este caso, Microsoft OneDrive.

Actualmente, la organización gestiona su documentación corporativa mediante un servidor local; sin embargo, no cuenta con una metodología formal estandarizada que regule aspectos como el acceso, el control de versiones, la seguridad y la recuperación de la información. Esta situación genera riesgos legales relacionados con la posible pérdida de datos, accesos no autorizados y la falta de trazabilidad documental, lo que puede afectar el cumplimiento normativo y la seguridad corporativa.

Para el desarrollo del proyecto, se requiere el cumplimiento de las normativas legales vinculadas con la protección de la información, la confidencialidad de los datos y los derechos de acceso, así como la alineación con estándares internacionales como ISO 27001, ISO 9001 e ITIL. Además, se establece que la solución propuesta debe respetar las políticas internas de la empresa y las condiciones contractuales establecidas con los proveedores tecnológicos.

Finalmente, la implementación de una metodología de gestión documental basada en OneDrive representa una oportunidad significativa para la organización, ya que permite reducir riesgos legales y mejorar la protección de la información corporativa. Asimismo, facilita la auditoría de documentos, la trazabilidad de los cambios y el control de accesos, contribuyendo de manera directa al cumplimiento de las obligaciones legales y contractuales de la empresa.

Proyecciones

Alcance Funcional

El alcance funcional del proyecto define los principales componentes y controles que formarán parte de la metodología propuesta para la gestión documental en la nube de la empresa Golden Comunicaciones S.A. En esta sección se describen los apartados funcionales que permitirán mejorar el control, la seguridad y la administración de los documentos corporativos mediante el uso de Microsoft OneDrive.

Estos apartados incluyen mecanismos de control de versiones, gestión de permisos, automatización de respaldos, controles de seguridad y lineamientos basados en buenas prácticas internacionales como ISO 27001 e ITIL. A continuación, en la Tabla 2, se presentan los apartados funcionales aprobados por la dirección de la empresa y una breve descripción de cada uno de ellos.

Tabla 2

Apartado aprobado por dirección

	Nombre del apartado	Descripción del apartado
Controles de bloqueo	**a) Edición colaborativa en tiempo real y control de versiones.**	Implementar una plataforma de colaboración en la nube, como Microsoft 365, esto con el fin de generar versiones guardadas en una línea del tiempo que permite restaurar cambios anteriores.
	b) Permisos de acceso de roles personalizados.	Configurar roles específicos para cada usuario, como editor, revisor o lector, ayuda a prevenir conflictos y a coordinar el trabajo colaborativo.
	c) Automatización de sincronización y respaldo	Automatizar el proceso de sincronización de archivos y carpetas en la nube.
Control de daños	**a) Respaldo automático y continuo.**	Implementar un sistema en la nube con respaldo automático, asegurando que los archivos se respalden continua y periódicamente.
	b) **Control de versiones y restauración de archivos.**	Se desarrollará una normativa para la revisión de versiones en archivos; proporciona una forma rápida de restaurar la información perdida.
Controles de seguridad para manipulación de carpetas	**a) Controles de seguridad.**	Integrar los controles de seguridad a partir de un cuadro comparativo, identificando cada acción que se desea realizar, identificando la ISO 27001 - Gestión de la Seguridad de la Información.
	b) Autenticación para determinar los cambios registrados y los permisos dados por los usuarios.	Se creará un plan para la revisión de cambios en archivos y carpetas con el objetivo de proteger la información que manipule cada usuario y persona externa.
	c) Revisión periódica de los permisos existentes.	Se generará una revisión de verificación de los permisos existentes en cada usuario y/o persona externa que no tenga un acceso confiable y, de esta manera, una limpieza en caso de que las personas no tengan acceso porque ya no laboren en la compañía.
	d) Alertas de seguridad. S	e aplicarán configuraciones que permitan detectar vínculos sospechosos a sitios web o mala manipulación de la información, activación de notificaciones para recibir alertas de seguridad.

	Nombre del apartado	Descripción del apartado
ITIIL - Gestión de Configuraciones y Activos de Servicio		Elaborar una política que incluya un marco para la gestión y control de configuraciones y activos con mayor flexibilidad y enfoque práctico: a) Centralización de la gestión. b) Automatización de procesos. c) Auditoría y control.
	a) Implementación de control de versiones.	Configurar la plataforma de nube para que mantenga un historial de cada archivo.
	b) Capacitación del personal.	Formar a los empleados en el uso seguro y correcto de la nube, destacando la importancia de seguir los protocolos de acceso y edición.

Nota. Propuesta para optimización en gestión de documentación para Golden Comunicaciones S.A. ubicada de San José.

Alcance Metodológico

Método Utilizado para el Desarrollo

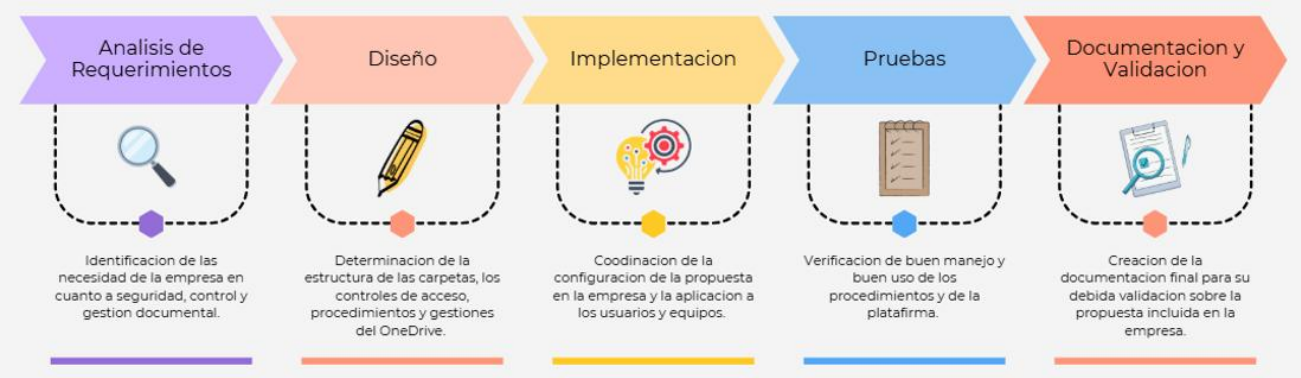
Para el desarrollo de la presente investigación se utilizará un método descriptivo aplicado, el cual permite analizar la situación actual de la manipulación y gestión documental de la empresa, así como proponer una solución orientada a la mejora de los procesos existentes.

El enfoque aplicado del método facilita la formulación de una metodología de gestión documental basada en Microsoft OneDrive, alineada con buenas prácticas internacionales, lo que permite que los resultados de la investigación sean directamente utilizables por la empresa. De acuerdo con Arias (2012), la investigación aplicada tiene como finalidad generar conocimientos orientados a la solución de problemas prácticos y específicos, lo cual se ajusta a los objetivos planteados en este estudio.

Ciclo de Vida del Software

Figura 1

Ciclo de Vida



Nota. Elaboración propia en Canva.

Alcance Tecnológico

El desarrollo de la investigación se apoya en el uso de tecnologías de la nube, en este caso sería la plataforma de Microsoft OneDrive, la cual se integra al sistema de Microsoft 365. Esto permite el almacenamiento, la gestión y el control de todas las versiones para la proyección corporativa que se desea integrar sin la necesidad de un sistema o software adicional, ya que se aprovechan las funcionalidades ya disponibles en la plataforma.

No se requiere el desarrollo de una aplicación web propia, ya que la investigación se centra en el diseño de una metodología de gestión documental, así como en la definición de procedimientos y controles operativos donde se usan herramientas existentes en OneDrive. El acceso a la plataforma se realiza mediante navegadores web y aplicaciones de escritorio proporcionadas por Microsoft; esto facilita a los usuarios su uso.

Asimismo, no requiere la implementación de servidores locales para el desarrollo del prototipo, debido a que el almacenamiento, el procesamiento y el respaldo de la información se realizan en la infraestructura en la nube de Microsoft. Esto permite reducir costos adicionales de hardware, el mantenimiento de equipos y los riesgos propensos a los servidores locales.

Finalmente, la investigación se apoya completamente en servicios en la nube, la solución ofrece disponibilidad, escalabilidad, control de accesos, auditoría de cambios y mecanismos de recuperación de información, lo que garantiza el cumplimiento de los lineamientos de seguridad.

CAPÍTULO II: MARCO REFERENCIAL

Construcción de la Perspectiva Teórica

De acuerdo con Hernández et al. (2017), “El marco teórico implica analizar y exponer de una manera organizada las teorías, investigaciones y los antecedentes en general que se consideren válidos y adecuados para encuadrar y orientar el estudio” (p.58). Este proceso permite fundamentar científicamente la investigación y detener el problema dentro del contexto académico. El marco referencial orienta el proceso de la investigación para llevar a cabo la finalización de la implementación de la propuesta en la empresa Golden Comunicaciones. También facilita la comprensión de los conceptos calve y se respalda en la toma de decisiones metodológicas duranta el desarrollo de la investigación.

La problemática identificada en Golden Comunicaciones está relacionada con las deficiencias en la gestión documental digital, la perdida de información, los bloqueos de archivos y el bajo rendimiento administrativo. Su análisis puede vincularse a la gestión inadecuada de la información, la ausencia de un sistema organizado y el uso limitado de tecnologías apropiadas. Estas situaciones generan retrasos en los procesos internos y afectan la eficiencia del equipo de trabajo, además, se evidencia la necesidad de modernizar la infraestructura tecnológica para garantizar mayor estabilidad operativa.

Según Hernadez et al. (2017):

> El marco teórico cumple diversas funciones dentro de una investigación: ayuda a prevenir errores que se han cometido en otros estudios, orienta sobre cómo habrá de realizarse el estudio, amplía el horizonte del investigador y conduce al establecimiento de hipótesis o afirmaciones que más tarde deberán someterse a prueba. (p. 58).

Por lo anterior, se hace referencia a que la situación actual de la empresa evidencia una necesidad de transformar el modelo y la forma de almacenar y administrar la documentación. Es por ello por lo que se justifica científicamente el desarrollo de una propuesta basada en herramientas tecnológicas más eficientes y actualizadas; esta transformación busca mejorar la organización interna y reducir los errores operativos. Además, pretende fortalecer la seguridad y disponibilidad de la información corporativa.

Gestión Documental, Seguridad de la Información y Normas Internacionales

Golden Comunicaciones S.A. presenta una dependencia de un servidor NAS ubicado en otro país, lo que incrementa la vulnerabilidad operativa y afecta la disponibilidad y accesibilidad de la información. Para mitigar esta situación, pueden aplicarse los principios establecidos en la norma ISO 27001, la cual dispone que la información debe protegerse con base en tres principios fundamentales que garantizan que los datos estén protegidos contra accesos no autorizados y pérdidas accidentales. Su aplicación permitirá fortalecer la estructura de seguridad de la empresa:

a) Confidencialidad.
b) Integridad.
c) Disponibilidad

La norma ISO 9001:2015 establece que las organizaciones deben garantizar un control adecuado sobre la información documentada para un eficaz trabajo en el sistema de gestión de calidad (ISO 2015). La falta de control de versiones de los archivos y los problemas que surgen cuando varias personas trabajan simultáneamente en un mismo documento evidencian un incumplimiento parcial de esta norma. Esto puede generar errores en los documentos y afectar la trazabilidad de la información.

Computación en la Nube como Modelo de Transformación Digital

Para Golden Comunicaciones S.A., la migración a una plataforma como Microsoft OneDrive representa una alternativa importante con soluciones eficientes, lo que permite:

a) Control de versiones.
b) Acceso seguro desde múltiples ubicaciones.
c) Gestión de permisos.
d) Copias de seguridad automáticas.
e) Alta disponibilidad para los usuarios.

Microsoft OneDrive protege los datos tanto en tránsito como en reposo. Además, dispone de autenticación de multifactor y herramientas de recuperación ante incidentes; estas características fortalecen la seguridad de la empresa de los datos de cada colaborador, ofrece mecanismos de sincronización automática que minimizan el riesgo de pérdida de información. Esto permite mantener la continuidad operativa incluso ante fallos técnicos o errores humanos.

Un enfoque planteado por Hernández et al. (2017) establece que la investigación aplicada busca la solución de problemas prácticos mediante la implementación de la mejora de procesos a través de una solución estructurada. En este contexto, la propuesta tecnológica no solo responde a una necesidad operativa, sino también a un fundamento metodológico sólido; la aplicación permite obtener resultados medibles y verificables. De esta manera, la investigación contribuye directamente al fortalecimiento organizacional.

Se pretende implementar un acceso seguro y una mayor estabilidad en la gestión de la información, de manera que los usuarios puedan manipular los archivos o carpetas con mayor seguridad. Asimismo, se incorpora un control de versiones que permita recuperar la información en caso de pérdida ocasionada por una mala manipulación por parte de algún colaborador. De igual manera, la gestión eficiente de permisos garantiza que no existan accesos inválidos o ingresos de externos a la información y archivos de la empresa. Finalmente, se espera que favorezca la obtención de mejores resultados, una reducción de errores operativos y una mejora en el desempeño laboral, trabajo en equipo eficiente, facilidad de entrega inmediata de archivos o documentación importante a la hora de una auditoría y crecimiento de mejoría en organización de datos.

Implicaciones del Estudio

La implementación de una metodología de gestión documental en la nube, basada en Microsoft OneDrive y alineada con las normas ISO 27001, ISO 9001, tiene las siguientes implicaciones:

a) Mejora de la disponibilidad y acceso remoto seguro a la información.
b) Reducción de conflictos de versiones y bloqueos de archivos.
c) Disminución de riesgo de pérdida de información.
d) Incremento en la productividad administrativa.

De acuerdo con Porter (1985), la eficiencia operativa sostenida puede convertirse en una ventaja competitiva cuando genera recursos y reduce costos. En este caso, la modernización del sistema documental impacta directamente en la competitividad de Golden Comunicaciones S.A. dentro del sector de telecomunicaciones. Asimismo, una gestión más eficiente de la información puede traducirse en mejores tiempos de respuesta al cliente, lo que favorece el posicionamiento de la empresa frente a sus competidores.

En Golden Comunicaciones, la aplicación de los fundamentos de la teoría de investigación permitió convertir una problemática tecnológica en un proyecto de indagación que se estructuró satisfactoriamente; esta transformación evidencia la importancia de la investigación aplicada en la solución de problemas empresariales. El proyecto no solo busca optimizar los procesos técnicos, sino también un fortalecimiento organizacional integral. De esta forma, se establece una base sólida para la mejora continua dentro de la empresa.

Arquitectura del Sistema

Con base en el análisis teórico y en el objetivo de la investigación, la arquitectura más adecuada corresponde al entorno computacional en la nube, ya que la implementación de Microsoft OneDrive como sistema central de almacenamiento y gestión documental constituye la alternativa más adecuada. Se contempla una fase de transición que consiste en mantener temporalmente el servidor NAS mientras se realiza la migración controlada de la información. Este proceso permitirá minimizar riesgos y asegurar la continuidad operativa. La planificación adecuada de esta transición será clave para el éxito del proyecto

El análisis realizado demuestra que la problemática de Golden Comunicaciones S.A. no es únicamente tecnológica, sino también estructural. La dependencia de una arquitectura centralizada tradicional ha generado vulnerabilidades que afectan la productividad. Además, limita la capacidad de adaptación ante cambios tecnológicos. Por ello, resulta necesario replantear el modelo de infraestructura para hacerlo más flexible y eficiente.

La adopción de la arquitectura en la nube representa una solución coherente y un avance operacional positivo para la empresa. Esta decisión se alinea con los objetivos estratégicos de mejora y modernización institucional. Asimismo, facilita la escalabilidad del sistema conforme la empresa crezca. De esta manera, se dispone de una infraestructura preparada para responder a futuros requerimientos tecnológicos.

Esta arquitectura en la nube puede complementarse con un modelo híbrido que combine recursos físicos y virtuales. Parte de la información puede mantenerse en servidores internos mientras otra se gestiona en la nube, garantizando mayor flexibilidad. Este enfoque permite conservar un nivel de control directo sobre datos sensibles. Además, facilita una transición gradual hacia un entorno completamente digitalizado.

Tecnologías Aplicables en la Investigación

De acuerdo con Hernández et al. (2017), toda la investigación aplicada debe apoyarse en herramientas y procedimientos que permitan resolver un problema práctico mediante un conocimiento sistemático. En este contexto, la tecnología se convierte en un elemento estratégico para el desarrollo del estudio y en un componente fundamental para la implementación de soluciones eficientes. Entre las principales tecnologías aplicables se encuentran las siguientes:

a) **Computación en la Nube: P**ermite almacenar y gestionar la información en servidores o estancias remotas que son accesibles mediante internet, reducción la dependencia de un servidor local. Asimismo, facilita la escalabilidad, el acceso remoto y la optimización de recursos tecnológicos, disminuyendo los costos de mantenimiento de la infraestructura física y mejora la disponibilidad del servicio.

b) **Microsoft OneDrive:** Se propone como plataforma principal para implementar el control automático de las versiones de las aplicaciones utilizadas diariamente por los colaboradores. Además de la administración centralizada de permisos, la recuperación de archivos eliminados o dañados, una sincronización en tiempo real y acceso desde múltiples dispositivos y equipos desde diferentes lugares.

c) **Herramientas de Respaldo Automático:** Permiten garantizar la continuidad operativa ante fallos técnicos o errores humanos, ya que aseguras copias actualizadas de la información en todo momento. Además, facilitan la recuperación rápida de datos ante incidentes inesperados. De esta manera, se reduce significativamente el impacto de posibles pérdidas de información en la empresa.

Antecedentes Investigativos

La transformación digital y la adopción de soluciones en la nube han sido ampliamente estudiadas en el ámbito organizacional debido a su contribución en la optimización de procesos internos y la mejora en la gestión de la información. Es por ello que la migración hacia plataformas colaborativas como OneDrive no solo responde a una necesidad técnica, sino también a una tendencia global de modernización empresarial.

Por otra parte, diversos estudios sobre gestión documental digital indican que una adecuada administración de la información contribuye significativamente a la reducción de errores administrativos y al mejoramiento del desempeño organizacional. Estos aportes permiten

comprender que la problemática de Golden Comunicaciones S.A. no es un caso aislado, sino parte de una tendencia organizacional más amplia. Por tanto, el análisis de antecedentes fortalece la justificación científica de la propuesta tecnológica planteada en esta investigación.

Definición de conceptos fundamentales

Para una mejor comprensión de la investigación, es necesario definir algunos conceptos clave que sustentan la investigación. En este sentido, la gestión documental se refiere al conjunto de procedimientos destinados a controlar la creación, almacenamiento, organización y disposición de documentos dentro de la organización. Según la ISO 9001:2015, “la información documentada para así asegurarse de que se encuentra disponible cuando sea necesario y que esto es adecuado para su utilización”: (párr. 10).

Por su parte, la seguridad de la información, conforme a la ISO 27001, exige “diseñar e implementar un conjunto coherente e integral de controles de seguridad de la información y/u otras formas de tratamiento de riesgos (como la evitación de riesgos o la transferencia de riesgos)” (párr. 5). Estos principios garantizan que la información esté protegida contra accesos no autorizados, alteraciones indebidas o pérdidas.

La computación en la nube es definida por Mell y Grance (2011) como “un modelo que permite el acceso a la red, práctico y bajo demanda, a un conjunto compartido de recursos informáticos configurables, por ejemplo, redes, servidores, almacenamiento y servicios”: (párr. 1). Este modelo reducirá la dependencia de la infraestructura física local y mejorará la escalabilidad de los servicios tecnológicos.

Finalmente, la arquitectura híbrida combina una infraestructura local con servicios en la nube, permitiendo mayor flexibilidad y control sobre la información. Este enfoque facilitará procesos de transición tecnológica y disminuirá los riesgos durante la migración de los datos.

Análisis de Riesgos Tecnológicos

Toda transformación digital implica riesgos que deben ser evaluados estratégicamente. Según ISO 27001:2013, la gestión de riesgos constituye un proceso continuo que permite identificar amenazas, evaluar vulnerabilidades y aplicar controles adecuados. En el caso de Golden Comunicaciones S. A., los riesgos pueden incluir fallas en la migración de datos, dependencia del proveedor de servicios en la nube y accesos no autorizados.

La dependencia de infraestructura ubicada en otro país incrementa la vulnerabilidad operativa y dificulta la recuperación inmediata ante incidentes. La evaluación de estos riesgos permite sustentar la necesidad de migrar hacia una arquitectura en la nube con mayores mecanismos de respaldo y seguridad. Así, la propuesta tecnológica se fundamenta no solo en eficiencia, sino también en prevención y control de riesgos.

En Costa Rica, Artavia (2025) indica que la gestión de vulnerabilidades mediante controles formales, como gestión de accesos y protección de datos, permite minimizar las exposiciones a ataques y riesgos informáticos. Este análisis de riesgos fortalece la propuesta investigativa, ya que evidencia una evaluación integral de la solución planteada y no se limita a destacar sus beneficios operativos.

Relación entre Transformación Digital y Competitividad

La transformación digital se ha convertido en un factor determinante para la competitividad empresarial. En este sentido, la modernización del sistema documental impacta directamente en la eficiencia administrativa y en la capacidad de respuesta ante los clientes y las auditorías. En consecuencia, esta transformación no solo responde a una necesidad operativa, sino también estratégica. De este modo, la implementación tecnológica se convierte en una venta estratégica sustentada en fundamentos teóricos.

La implementación de Microsoft OneDrive dentro de una arquitectura en la nube no debe interpretarse únicamente como una mejora técnica; debe ser una estrategia organizacional orientada a la sostenibilidad y crecimiento en Golden Comunicaciones S.A.

Desde el enfoque de competitividad, Martínez (2018) señala que la incorporación de tecnología e innovación en los procesos productivos es determinante para mejorar la productividad y el posicionamiento de las empresas en economías abiertas como la costarricense. En un entorno caracterizado por alta competencia y rápida evolución tecnológica, las organizaciones que adoptan herramientas digitales desarrollan una mayor capacidad de respuesta ante cambios del mercado. En el caso de Golden Comunicaciones S.A., la implementación de una arquitectura en la nube fortalece la agilidad organizacional y reduce tiempos de operación. Esto repercute positivamente en la calidad del servicio ofrecido y en la percepción del cliente. Así, la transformación digital se traduce en una ventaja competitiva sostenible.

La evidencia teórica, tanto nacional como internacional, respalda que la innovación tecnológica incide directamente en el desempeño empresarial. En consecuencia, la transformación digital en Golden Comunicaciones S.A. no solo responde a una necesidad operativa inmediata, sino que constituye una decisión estratégica orientada a consolidar ventajas competitivas sostenibles en el contexto costarricense.

CAPÍTULO III: MARCO METODOLÓGICO

Enfoques de Investigación

Los enfoques de investigación constituyen la orientación metodológica que guía el proceso científico y determinan la forma en la que se recolectan, analizan e interpretan los datos. Según Hernández et al. (2017), "Los métodos de investigación son los distintos caminos propuestos para hacer investigación y lograr el conocimiento científico considerado como valido." (p.21).

Existen tres enfoques principales: cuantitativo, cualitativo y mixto. Cada uno posee características particulares, y su elección depende de la naturaleza del problema y de los objetivos planteados. En esta investigación se analizan los tres enfoques con el propósito de determinar cuál se ajusta mejor a la propuesta metodológica para Golden Comunicaciones S.A.

Enfoque Cuantitativo

El enfoque cuantitativo se fundamenta en la medición numérica y el análisis estadístico para comprobar hipótesis previamente establecidas. De acuerdo con Hernández et al. (2017), "Este método se utiliza principalmente en las ciencias formales (como las matemáticas y la lógica)" (p. 21). En el contexto de la investigación, permitirá medir la frecuencia de errores documentales, los tiempos de acceso y las pérdidas de información. Además, facilita la obtención de indicadores concretos sobre productividad y eficiencia administrativa.

Enfoque Cualitativo

El enfoque cualitativo puede utilizarse para obtener información detallada sobre un problema o generar nuevas ideas para la investigación. Este enfoque facilita la exploración de experiencias, percepciones y significados mediante técnicas como entrevistas, observación y análisis documental. Para Golden Comunicaciones S.A., será útil para comprender cómo los colaboradores perciben los problemas del servidor NAS y la transición hacia la nube.

Enfoque Mixto

El enfoque mixto combina elementos cuantitativos y cualitativos en un mismo estudio, integrando medición estadística y análisis interpretativo. Hernández et al. (2017) señalan que a este enfoque "se les llama investigación integrativa, multimodos, métodos múltiples, estudios de triangulación e investigación mixta". (p.22). En la presente investigación, el enfoque mixto posibilitaría medir la reducción de errores documentales y, simultáneamente, analizar la

percepción de los usuarios sobre la nueva metodología. Además, fortalece la validez del estudio al triangular la información obtenida. Este enfoque resulta particularmente útil en proyectos aplicados con impacto organizacional.

Enfoque de Investigación Seleccionado

Para el desarrollo del presente proyecto se selecciona el enfoque mixto, debido a que la problemática identificada requiere tanto medición objetiva como análisis interpretativo. La propuesta de migración hacia Microsoft OneDrive implica evaluar indicadores cuantificables como tiempos de acceso, número de incidencias y control de versiones. Sin embargo, también se podría comprender la percepción de los colaboradores respecto a la seguridad y facilidad de uso de la plataforma. Esta combinación fortalece la toma de decisiones metodológicas en Golden Comunicaciones S.A., y garantiza resultados medibles y contextualizados que respalden la viabilidad de la propuesta tecnológica.

Además de medir indicadores objetivos, resulta necesario comprender la experiencia de los colaboradores con el uso del sistema actual y durante la implementación de la nueva plataforma. La integración de ambos enfoques permite diseñar una metodología fundamentada en datos verificables y en la realidad organizacional. Esta decisión se alinea con lo expuesto por Hernández et al. (2014), quienes destacan que el enfoque mixto proporciona una perspectiva integral del fenómeno estudiado.

Tipos de Investigación

Los tipos de investigación se refieren al alcance que tendrá el estudio de acuerdo con sus objetivos y el nivel de profundidad con el que se aborde el objeto de estudio. Según Hernández et al. (2017), “dependen de los objetivos del investigador para combinar los elementos del estudio” (p. 73). Cada tipo responde a diferentes propósitos específicos dentro del proceso científico, por lo que su selección depende del grado de conocimiento previo sobre el problema. En la presente investigación se analizan tres tipos principales para determinar cuál se ajusta mejor a la propuesta.

De acuerdo con Hernández et al. (2017), “los cuatro alcances del proceso de la investigación son igualmente válidos e importantes y han contribuido al avance de las ciencias. Cada uno tiene sus objetivos y razón de ser” (p. 80). A partir de este planteamiento, se examinan los tipos de investigación que fundamentan el presente estudio.

Investigación Exploratoria

La investigación exploratoria tiene como objetivo examinar un problema poco estudiado o sobre el cual existe escasa información. En el caso de Golden Comunicaciones S.A., la migración metodológica hacia la nube representa un proceso novedoso dentro de la empresa. Por ello, este tipo de investigación permite comprender inicialmente la problemática y definir los lineamientos de la propuesta.

Al respecto, Hernández et al. (2017) señalan lo siguiente:

> Sirven para familiarizarnos con problemas que no se conocen o de los cuales se sabe poco, obtener información sobre la posibilidad de llevar a cabo una investigación más completa respecto de un contexto particular, indagar nuevos problemas, identificar conceptos o variables promisorias, establecer prioridades para investigaciones futuras o proponer afirmaciones y postulados. (p. 75).

Investigación Descriptiva

Busca especificar propiedades y características relevantes del fenómeno que se analice, detalla cómo se manifiesta el problema en la organización. En la investigación se describen errores de bloqueo, la pérdida de información y las fallas de acceso remoto asociados al servidor NAS. Este tipo de investigación posibilita documentar la situación actual de la empresa y ofrece un diagnóstico estructurado de la problemática. Asimismo, proporciona una base sólida para la formulación en la propuesta.

Según Hernández et al. (2017), “en estos estudios, el investigador debe ser capaz de definir, o al menos visualizar, qué medirá (qué conceptos, variables, componentes, etc.) y sobre qué o quiénes recolectará los datos (personas, grupos, comunidades, objetos, animales, hechos, empresas)” (p. 77).

En la presente investigación se establecen objetivos orientados a identificar las deficiencias derivadas del uso del servidor NAS y lo que conlleva tener bajo rendimiento administrativo; se evaluarán las mejores variables y componentes para adecuar la plataforma de Microsoft OneDrive y que cada usuario tenga un concepto claro y estable para su debida manipulación.

Investigación Explicativa

Hernández et al. (2017) señalan que los estudios explicativos "son más que la descripción de conceptos o fenómenos o el establecimiento de relaciones entre variables; más bien, están diseñados para determinar las causas de los eventos y fenómenos físicos o sociales" (p. 78).

La investigación explicativa tiene como propósito establecer relaciones de causa y efecto entre variables, lo que permite analizar por qué ocurren los problemas en la gestión documental. En el caso de Golden Comunicaciones S.A., este tipo de investigación posibilita identificar cómo la dependencia del servidor NAS incide en la gestión documental y limita la gestión y la creación de documentación y en la pérdida de productividad.

Investigación Correlacional

La investigación correlacional tiene como propósito identificar la relación o grado de asociación que existe entre dos o más variables dentro de un contexto determinado. Hernández et al. (2017) señalan que "Las correlaciones pueden ser positivas (directamente proporcionales) o negativas (inversamente proporcionales). Si es positiva, significa que los casos que muestren altos valores en una variable tenderán también a manifestar valores elevados en la otra variable." (p. 78).

En el caso de Golden Comunicaciones S.A., este tipo de investigación permitiría analizar la relación entre la frecuencia de fallas del servidor NAS y el nivel de productividad administrativa, esto medirá estadísticamente cómo ciertos problemas tecnológicos se asocian con el rendimiento laboral y cómo la migración hacia Microsoft OneDrive sería la mejor opción a nivel empresarial.

Tipo de Investigación Seleccionado

Para esta investigación, el tipo de investigación seleccionado es descriptivo con alcance aplicado, ya que se centra en analizar y detallar una situación concreta dentro de la organización. El estudio no pretende establecer relaciones entre variables ni explicar causas profundas con pruebas experimentales; por el contrario, se pretende plantear mejoras prácticas que permitan optimizar la gestión de la información.

Con base en este análisis, la investigación se orienta a:

a) Analizar la situación actual del sistema documental.
b) Describir los problemas existentes (bloqueos, pérdida de información, fallas de acceso).

c) Propones una solución metodológica basada en Microsoft OneDrive.
d) Aplicar buenas prácticas como ISO 27001 e ISO 9001.

Según Hernández et al. (2017), “los estudios descriptivos buscan especificar las propiedades, características y perfiles de personas, grupos, comunidades, procesos u objetos” (p. 76). Este planteamiento es coherente con la investigación, porque estás describiendo cómo funciona actualmente la gestión documental y cómo debe estructurarse una nueva metodología. En consecuencia, el estudio permite fundamentar la propuesta de mejora con base en el análisis previamente expuesto.

Fuentes de Información

Fuentes de Información Primaria

Según Editorial Etecé (2025), estas fuentes “Son las más directas respecto al elemento investigado”; es decir, corresponde a información obtenida directamente de la realidad organizacional de Golden Comunicaciones S.A.

En esta investigación se utilizarán las siguientes fuentes primarias:

a) Entrevistas semiestructuradas al personal administrativo y técnico.
b) Encuestas estructuradas para medir la frecuencia de errores y la percepción del sistema.
c) Observación directa del uso del servidor NAS y la nueva plataforma, Microsoft OneDrive.
d) Revisión de registros internos de incidencias.

Estas fuentes permitirán analizar bloqueos de archivos, pérdidas de información y problemas de acceso remoto.

Fuentes de Información Secundaria

Las fuentes de información secundaria son aquellos documentos que interpretan, analizan, organizan o explican información proveniente de fuentes primarias. Su función principal es ofrecer una visión más elaborada y estructurada sobre un tema determinado, facilitando la comprensión y el análisis crítico.

En el presente documento, estas fuentes corresponden a libros especializados, normas técnicas, artículos académicos y publicaciones científicas relacionadas con la gestión documental

y la seguridad de la información. En el documento corresponden a libros, normas, artículos académicos y publicaciones especializadas.

Libros y Autores Académicos

a) Hernández Sampieri, R., Méndez Valencia, S., Mendoza Torres, C. P., & Cuevas Romo, A. (2017). Fundamentos de investigación. McGraw-Hill Education.
b) Porter, M. (1985). Competitive Advantage. Free Press.
c) Martínez Piva, J. M. (2008). Generación y protección del conocimiento. CEPAL.
d) **Normas y Estándares Internacionales**

a) ISO/IEC 27001:2013 – Seguridad de la información.
b) ISO 9001:2015 – Gestión de calidad.
c) International Organization for Standardization (ISO) (2013).

Artículos y Documentos Técnicos

a) Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST.
b) Artavia López, L. I. (2025). Gestión de vulnerabilidades según ISO 27001.
c) ESGinnova Group (2026). Información documentada ISO 9001.
d) Glosario HPE (2025). Arquitectura de nube.
e) Wikipedia (2022). ISO/IEC 27001.

Fuentes de Información Terciaria

Según Editorial Etece (2025), las fuentes terciarias “son las que elaboras a partir de las fuentes primarias y secundarias”. (s.p). Esto significa que constituyen una recopilación o síntesis de información proveniente de testimonios e interpretaciones. Si el evento es un hecho histórico, la fuente terciaria puede ser un protocolo que se elabora a partir de las fuentes secundarias.

En el caso de Golden Comunicaciones S.A., las fuentes terciarias cumplen un papel fundamental en la estructuración teórica y normativa, ya que pueden llegar a facilitar la ubicación de normativa internacional aplicable y fortalecen el acceso a referencias relacionadas con estándares oficiales sin necesidad de adquirir documentos completos.

Variables

Las variables de la investigación representan los elementos fundamentales que permiten analizar y comprender la problemática relacionada con la gestión documental en la empresa Golden Comunicaciones S.A. Estas variables se establecen con el propósito de evaluar aspectos

clave vinculados con el control, la seguridad y la administración de la información dentro del sistema de almacenamiento digital que será utilizado por la organización.

Variables Conceptuales

Las variables conceptuales definen el significado teórico de cada variable dentro del estudio y explican la forma en la que se comprende cada concepto en el contexto de la investigación. En este proyecto las principales variables conceptuales son:

a) **Control de versiones:** Se entiende como el conjunto de mecanismos tecnológicos que permitirán registrar, almacenar y recuperar los cambios realizados en documentos digitales, garantizando la trazabilidad y restauración ante los errores.
b) **Control de accesos:** Es la gestión estructurada de los permisos y la autenticación que regula quién podrá visualizar, editar o eliminar documentos dentro de la plataforma en la nube.
c) **Seguridad de la información:** Es el conjunto de controles que se orientarán a proteger la información bajo principios de confidencialidad, integridad y disponibilidad.
d) **Recuperación de información:** En este caso es el procedimiento técnico que restaura documentos eliminados o modificados incorrectamente mediante respaldos automáticos y versiones históricas.

Variables Operacionales

Las variables operacionales corresponden a la forma en que los conceptos teóricos definidos en la investigación se traducen en elementos observables y medibles dentro del estudio. En otras palabras, permiten transformar los conceptos abstractos en indicadores concretos que pueden ser analizados mediante los instrumentos de recolección de datos.

Estas variables facilitan la evaluación objetiva del funcionamiento del sistema de gestión documental, así como la medición de los cambios o mejoras que se puedan obtener con la implementación de la metodología propuesta basada en Microsoft OneDrive.

Control de versiones:

a) Número de conflictos de edición detectados.
b) Cantidad de versiones almacenadas por archivo.

c) Tiempo requerido para restaurar una versión anterior.

Control de accesos:

a) Número de usuarios definidos por rol.
b) Frecuencia de versión de permisos.
c) Cantidad de cambios realizados en configuraciones de acceso.

Seguridad de la información:

a) Número de accesos no autorizados registrados.
b) Cantidad de incidentes reportados.
c) Activación de autenticación multifactorial.

Recuperación de información:

a) Tiempo promedio de restauración de archivos.
b) Número de archivos recuperados exitosamente.
c) Frecuencia de ejecución de respaldos automáticos.

Variables Instrumentales

Las variables instrumentales son relevantes dentro de la investigación, ya que son las que recogen los datos necesarios para medir las variables operacionales. Para este estudio, se utiliza una encuesta estructurada para medir la percepción de seguridad, la frecuencia de errores y el nivel de satisfacción con el sistema actual y el propuesto para Golden Comunicaciones S. A. Se realiza una entrevista semiestructurada para analizar la experiencia de los colaboradores con el servidor NAS, una opción sobre la migración a Microsoft OneDrive, esto para tener la percepción de mejora en productividad.

Finalizando, se realiza una observación directa para registrar el tiempo de acceso a los archivos, los bloqueos de documentos y las fallas de sincronización; asimismo, se dispondrá una revisión documental con bitácoras en el sistema para obtener un registro de incidencias, el historial de todas las versiones y tener reportes de auditoría y accesos.

Tabla 3

Variables de investigación

Objetivo Específico	Variable	Variable Conceptual	Variable Instrumental	Variable Operacional
Crear controles de bloqueo para evitar errores en archivos.	Control de versiones.	Conjunto de mecanismos que permiten registrar, almacenar y restaurar versiones anteriores de un documento.	Número de conflictos de edición, cantidad de versiones registradas por archivo.	Entrevista estructurada. Registro de incidencias del sistema.
Elaborar procedimientos que controlen los daños generados por usuarios.	Seguridad documental.	Conjunto de políticas y controles destinados a proteger la información contra accesos no autorizados o alteraciones indebidas.	Cantidad de accesos no autorizados detectados, número de incidentes reportados.	Entrevista semiestructurada Bitácora de accesos
Elaborar controles de seguridad en el acceso a carpetas.	Control de accesos	Gestión de permisos y autenticación para regular el acceso a la información.	Número de usuarios con permisos definidos por rol, frecuencia de cambios en permisos.	Observación directa Revisión de configuración en OneDrive
Implementar un plan de recuperación y control de versiones.	Recuperación de la información.	Procedimiento que permite restaurar documentos eliminados o modificados incorrectamente	Tiempo promedio de restauración de archivos, cantidad de archivos recuperados exitosamente.	Registro técnico Reportes del sistema.

Nota. Elaboración propia, 2026.

Población

La población constituye el conjunto total de elementos que poseen características comunes y que son objeto del estudio dentro del contexto de una investigación. En este caso, la población está conformada por todos los colaboradores de Golden Comunicaciones S. A., que interactúan directa o indirectamente con el sistema de gestión documental de la empresa, ya sea mediante el servidor NAS actual o a través de la futura implementación de Microsoft OneDrive.

La población presenta las siguientes características:

a) Colaboradores administrativos.
b) Personal técnico de campo.
c) Departamento de tecnologías de información (TI).
d) Usuarios con acceso a carpetas compartidas.
e) Personal que utiliza documentos de Word, Excel y PowerPoint corporativos.
f) Usuarios que requieren acceso remoto mediante VPN.

Todos estos colaboradores comparten una característica común, que se relaciona con la dependencia del sistema documental para realizar sus funciones laborales. Por esta razón, constituyen sujetos relevantes para analizar la problemática identificada, relacionada con bloqueos, pérdida de información, conflictos de edición y fallas de acceso remoto.

Según la información recopilada, la empresa cuenta aproximadamente con:

a) 12 equipos de cómputo activos
b) Personal administrativo y técnico que utiliza el servidor NAS.
c) Área de TI responsable del mantenimiento y supervisión

Por lo anterior, se estima que la población está conformada por entre 15 y 20 colaboradores activos que utilizan el sistema documental de manera contante. Debido a que se trata de una organización de tamaño pequeña o mediana, la población es finita y accesible, lo que facilita la recolección directa de información.

Muestra

En el contexto presente de la investigación, la muestra se define considerando a los colaboradores de la empresa Golden Comunicaciones S.A. que participan directamente en el manejo, almacenamiento y gestión de documentos digitales dentro de la organización. La selección de estos participantes resulta fundamental, ya que son los usuarios que interactúan de manera

constante con los sistemas de almacenamiento y control documental, por lo que su experiencia y conocimiento permiten obtener información relevante sobre las problemáticas existentes y las posibles mejoras que se pueden implementar en el sistema.

Según Hernández et al. (2017):

> Una muestra es un subgrupo de la población o universo que nos interesa, sobre el cual se recolectarán los datos pertinentes y deberá ser representativo de dicha población (de manera probabilística, para que podamos generalizar los resultados encontrados en la muestra a la población, o cualitativamente, para comenzar a conocer la población por medio de la muestra). (pp. 128-129).

En esta investigación, la muestra corresponde al grupo de colaboradores de Golden Comunicaciones S.A. que participa en la aplicación de los instrumentos de recolección de datos: encuestas, entrevistas y observación. Se emplea un muestreo probabilístico, específicamente el muestreo aleatorio simple, debido a que los colaboradores que utilizan el sistema documental tienen la misma probabilidad de ser seleccionados.

Cálculo de la Muestra

Los valores utilizados en la investigación se reflejan de la siguiente manera:

1. N = 20 colaboradores (población estimada)
2. Nivel de confianza = 95%.
3. Según la tabla proporcionada: K = 1.96
4. p = 0.5 (cuando no se conoce la proporción real)
5. q = 0.5
6. = 0.05 (5% margen de error)

Teniendo en cuenta la fórmula de cálculo tomada de la presentación en el taller de investigación se sustituye con los anteriores valores:

$$n = \frac{20(0.5)(0.5)(1.96)^2}{(0.05)^2(20-1) + (0.5)(0.5)(1.96)^2}$$

La muestra requerida es aproximadamente:

$$n \approx 19 colaboradores$$

Con la información anterior la población es de 20 colaboradores y la muestra es de 19, se define que estadísticamente es más conveniente aplicar un censo poblacional, es decir, incluir a todos los colaboradores. Esto elimina el error muestral y aumenta la confiabilidad del estudio.

Instrumentos de Recolección de Datos

Los instrumentos de recolección de datos constituyen las herramientas utilizadas en el proceso de investigación para obtener la información necesaria que permita analizar la problemática planteada y dar respuesta a los objetivos del estudio. A través de estos instrumentos se recopilan datos relevantes de manera sistemática y organizada, lo que facilita posteriormente su análisis e interpretación dentro del marco metodológico de la investigación.

En el desarrollo del presente estudio, los instrumentos seleccionados permiten obtener información directa sobre el manejo de la gestión documental dentro de la empresa Golden Comunicaciones S.A., así como identificar las principales dificultades relacionadas con el control de versiones, la seguridad de la información, el acceso a los documentos y los procesos de recuperación de archivos. La aplicación de estos instrumentos facilita la recopilación de datos tanto cualitativos como cuantitativos, permitiendo comprender la situación actual del sistema de gestión documental y evaluar posibles mejoras mediante la implementación de soluciones tecnológicas basadas en almacenamiento en la nube.

La Observación

La observación consiste en examinar atentamente un fenómeno, hecho o situación, con el propósito de recopilar información y registrarla para su posterior análisis. En la presente investigación, esta técnica es aplicada para el uso actual del servidor NAS y al funcionamiento posterior de la plataforma Microsoft OneDrive.

Durante el estudio se observa el uso del servidor NAS actual, el tiempo de acceso a archivos, conflictos de edición simultánea, bloqueos de documentos y fallas de sincronización. El objetivo consiste en identificar de manera directa las debilidades del sistema actual y comparar posteriormente con la solución propuesta de la nube.

La aplicación de esta técnica tiene como finalidad identificar los errores frecuentes en la manipulación de documentos y analizar el comportamiento de los usuarios ante conflictos de archivos; también se quiere medir tiempos reales de acceso y evaluar la eficiencia del sistema actual ante el modelo propuesto. Esto permitirá sustentar la necesidad de implementar una metodología estructurada basada en Microsoft OneDrive.

Para el análisis y la interpretación de los datos, se procede a clasificar incidencias por tipo, determinar patrones repetitivos y comparar los resultados antes y después de la implementación de la plataforma; esto permitirá justificar el procedimiento de migración a la nube.

Entrevista

En esta investigación, la entrevista permite conocer la percepción de los colaboradores de Golden Comunicaciones S.A. respecto al servidor NAS actual y la propuesta de migración hacia la nube. Esta técnica tiene el propósito obtener información detallada sobre la experiencia en el uso del sistema de gestión documental.

Se utiliza una entrevista semiestructurada, debido a que se cuenta con una guía de preguntas previamente elaboradas, permitiendo profundizar en respuestas relevantes y facilitando la obtención de información detallada sobre problemas específicos. La entrevista se aplica cuando sea necesario comprender la experiencia directa del colaborador con los bloqueos de archivos, la pérdida de información, fallas de sincronización y el uso de VPN para acceso remoto.

Asimismo, se analiza la percepción en el usuario y en la implementación sobre la seguridad documental que puede brindar la plataforma, la facilidad de acceso a la plataforma, el desarrollo de productividad administrativa al día a día y la confianza en la plataforma sobre la nube para la seguridad de la empresa y el colaborador.

Los resultados esperados sobre la entrevista es que se evidencie la necesidad de migración, se identifiquen las debilidades estructurales al tener el sistema de NAS, y se tenga información clave para diseñar la metodología de gestión documental.

Proceso para Recolección y Análisis de Datos

El proceso de recolección de la información se desarrolla de manera sistemática y organizada, iniciando con el diseño y validación de los instrumentos de investigación. Para ello, se elaboró un cuestionario estructurado compuesto por preguntas cerradas y abiertas, alineadas con

las variables del estudio relacionadas con el control de versiones, seguridad documental, accesibilidad y recuperación de información. Asimismo, se diseña una guía de entrevista semiestructurada que permitirá profundizar en la experiencia de los colaboradores respecto al sistema actual de almacenamiento. Ambos instrumentos serán revisados para garantizar coherencia con los objetivos específicos y claridad en su redacción.

Posteriormente, se determina la muestra tomando como base la población de colaboradores que utilizan el sistema de almacenamiento documental en la empresa. Una vez calculado el tamaño muestral mediante la fórmula estadística correspondiente, se seleccionan los participantes que forman parte del estudio. Este procedimiento permite asegurar que los datos recolectados representen adecuadamente la realidad organizacional y que los resultados obtenidos tengan validez dentro del contexto de la investigación.

El análisis de la información se desarrolla en dos niveles, el cuantitativo y el cualitativo. En el análisis cuantitativo se calcularán frecuencias, porcentajes y, cuando corresponda, medidas descriptivas que permitan identificar los problemas detectados en el sistema documental actual. Los resultados serán presentados mediante tablas y gráficos estadísticos que faciliten su comprensión. Por otra parte, el análisis cualitativo permite interpretar las experiencias y percepciones de los colaboradores, complementando los resultados numéricos con una visión más profunda del contexto organizacional.

CAPÍTULO IV: ANALISIS DE RESULTADOS

Entrevista

En este apartado se presentan los resultados obtenidos a partir de la aplicación de los instrumentos de recolección de datos, entre los cuales se incluye una entrevista y una observación directa dentro de la empresa Golden Comunicaciones S.A. El análisis se realiza en función de las variables definidas en capitulo metodológico: control de versiones, control de accesos, seguridad de la información y recuperación de la información.

Observación

La observación permite validar los resultados obtenidos en los instrumentos aplicados previamente. Durante el análisis del sistema actual se identificaron hallazgos como la presencia constante de bloqueos cuando varios usuarios acceden a un mismo archivo, la ausencia de control de versiones automatizado, procesos manuales para la recuperación de información, estructura desorganizada de carpetas y la falta de alertas de seguridad o notificaciones ante cambios.

Asimismo, se observó que el tiempo de acceso a los archivos depende en gran medida de la estabilidad de la red, lo que genera interrupciones en el flujo de trabajo.

Preguntas

Análisis de resultados de la entrevista a personal de la empresa Golden Comunicaciones S.A.

Perfil del entrevistado

Pregunta 1: Área en la que labora

Respuesta: Administrativo.

Pregunta 2: Tiempo laborado en la empresa

Respuesta: 4ª 6 años.

Pregunta 3: ¿Utiliza el sistema de almacenamiento de la empresa?

Respuesta: Sí

El análisis del perfil del entrevistado pertenece al área administrativa, lo cual resulta relevante porque tiene conocimiento directo del sistema actual y de sus limitaciones técnicas. Asimismo, el tiempo laboral indica experiencia suficiente para evaluar el funcionamiento del sistema y sus impactos en los procesos.

Pregunta 4: ¿Qué dificultades ha encontrado al trabajar con el sistema actual de almacenamiento documental?

Objetivo de la entrevista: Esta pregunta busca identificar las principales limitaciones del sistema actual desde la experiencia directa del colaborador. Se busca evidenciar problemas técnicos y operativos como lentitud, fallas de acceso, bloqueos de archivos o dependencia de la VPN. El objetivo es confirmar la existencia de una problemática real que justifique la necesidad de una mejora tecnológica.

Análisis de resultados de entrevista: Los resultados evidencian que el sistema presenta problemas de rendimiento y disponibilidad de la información. La lentitud en los accesos y los bloqueos archivos indican limitaciones técnicas del servidor, mientras que la dependencia de la VPN demuestra falta de accesibilidad remota eficiente. Estos hallazgos confirman que el sistema no responde a las necesidades actuales de trabajo flexible y colaborativo.

Pregunta 5: Describa una situación en la que haya tenido problemas al editar o compartir un documento con otros colaboradores.

Objetivo de la entrevista: Esta pregunta tiene como finalidad identificar problemas relacionados con el trabajo colaborativo y el control de versiones. Se pretende identificar situaciones reales en las que se presenten conflictos de edición, duplicidad de archivos o pérdida de información al compartir documentos entre colaboradores.

Análisis de resultados de entrevista: Los resultados identifican fallas críticas relacionadas con la integridad y disponibilidad de la información documental. La corrupción de archivos y la imposibilidad de acceso simultáneo evidencian la ausencia de control de versiones y colaboración en tiempo real. Esto genera confusión, pérdida de información y riesgos para la continuidad del trabajo.

Pregunta 6: ¿Cómo afecta el sistema actual su organización y gestión diaria de documentos?

Objetivo de la entrevista: El propósito de esta pregunta es determinar el impacto del sistema actual en la productividad diaria de los colaboradores. Se busca identificar si existen pérdidas de tiempo, desorganización documental o reprocesos que afecten el desempeño laboral.

Análisis de resultados de entrevista: Los resultados evidencian un impacto directo del siento actual sobre la productividad organizacional. La necesidad de rehacer documentos y la

espera por permisos demuestra procesos centralizados e ineficientes. Además, la dependencia de un único usuario externo limita la disponibilidad de la información y retrasa la gestión administrativa.

Pr***egunta 7: ¿Qué mejoras considera necesarias en el sistema de gestión documental de la empresa?***

Objetivo de la entrevista: El propósito de esta pregunta busca identificar las necesidades reales del usuario respecto a un sistema ideal de gestión documental. Se pretende evidenciar cuáles funcionalidades son prioritarias, como acceso remoto, control de permisos, respaldo automático y trabajo colaborativo.

Análisis de resultados de entrevista: Los resultados permiten identificar los requerimientos funcionales que el sistema actual no satisface. Entre las principales necesidades destaca el fortalecimiento de la seguridad, el control de accesos y el monitoreo de actividades, lo cual refuerza la necesidad de implementar una solución moderna de gestión documental.

Pregunta 8: ¿Qué expectativas tendría frente a un sistema en la nube?

Objetivo de la entrevista*:* El objetivo es conocer la percepción del colaborador ante la posible migración a la nube. Se pretende evidenciar el nivel de aceptación, confianza y beneficios esperados, como seguridad, rapidez y facilidad de acceso.

Análisis de resultados de entrevista: Los resultados muestran una percepción positiva hacia la migración a la nube. Las expectativas mencionadas coinciden con las ventajas de las plataformas modernas, lo que demuestra apertura al cambio tecnológico y confianza en sus beneficios.

Pregunta 9: ¿Considera que la empresa requiere capacitación en gestión documental digital? Explique por qué.

Objetivo de la entrevista: Esta pregunta busca determinar la necesidad de formación y sensibilización del personal en materia de gestión documental digital. Se pretende evidenciar la importancia de incluir capacitación como parte de la metodología propuesta para asegurar el uso adecuado del sistema.

Análisis de resultados de entrevista: Los datos obtenidos evidencian que el factor humano representa un riesgo en la gestión documental. La falta de conocimiento sobre buenas prácticas y manejo de errores refuerza la necesidad de incluir procesos de capacitación como parte de la propuesta.

Pregunta 10: ¿Desea agregar algún comentario adicional sobre el manejo actual de los documentos de la empresa?

Objetivo de la entrevista: Esta pregunta abierta tiene como objetivo obtener percepciones generales que no hayan sido contempladas en preguntas anteriores. Se pretende evidenciar la valoración global del sistema actual y reforzar la justificación de la propuesta de mejora.

Análisis de resultados de entrevista: La percepción global confirma que el sistema actual ha quedado desactualizado frente a las necesidades de la empresa. Se evidencia una clara necesidad de modernización tecnológica para mejorar la eficiencia, seguridad y disponibilidad de la información.

Conclusión del análisis de resultados

La entrevista realizada a una colaboradora del área administrativa de Golden Comunicaciones S.A. permitió conocer su experiencia con el sistema actual de gestión documental. Durante la conversación se identificaron dificultades relacionadas con la lentitud en el acceso, bloqueos de archivos, dependencia de la VPN, problemas al compartir y editar documentos y limitaciones en el control de versiones. También se señaló la necesidad de mejorar la seguridad, los permisos de acceso, los respaldos y la organización de la información.

Asimismo, la entrevistada mostró una percepción positiva hacia la implementación de una solución en la nube, destacando como beneficios esperados una mayor accesibilidad, seguridad y facilidad para trabajar con los documentos. Finalmente, se consideró necesaria la capacitación del personal para garantizar el uso adecuado de la nueva herramienta. Estos resultados respaldan la necesidad de modernizar la gestión documental de Golden Comunicaciones S.A.

CAPÍTULO V: PROPUESTA

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

FACULTAD DE INGENIERÍA INFORMÁTICA

TRABAJO FINAL DE GRADUACIÓN PARA OPTAR POR EL GRADO DE BACHILLERATO EN INGENERIA DE SOFTWARE

PROPUESTA DE UNA METODOLOGÍA PARA EL GESTIONAMIETO DE LA DOCUMENTACIÓN EN LA NUBE PARA GOLDEN COMUNICACIONES S.A

MARIA CAMILA FIGUEROA MORA

ABRIL, 2026

Introducción de la Propuesta

El presente capítulo desarrolla la propuesta metodológica orientada a optimizar la gestión documental en la nube para la empresa Golden Comunicaciones S.A. Como se evidenció en los capítulos anteriores, la organización presenta limitaciones relacionadas con el acceso remoto, la pérdida de información, los conflictos de versiones y la baja productividad administrativa, debido al uso de un servidor NAS ubicado en el extranjero. Estas condiciones justifican la necesidad de establecer una metodología estructurada que permita modernizar la administración de la información corporativa.

La propuesta se fundamenta en la implementación de una solución basada en Microsoft OneDrive, alineada con buenas prácticas internacionales de seguridad, calidad y gestión de servicios de TI. Esta iniciativa busca mejorar el control de acceso, la disponibilidad de la información, la trazabilidad documental y la continuidad operativa de la empresa. Asimismo, pretende facilitar el trabajo colaborativo y reducir los riesgos asociados al manejo manual de archivos.

En este capítulo se describen los elementos que conforman el prototipo propuesto, incluyendo el análisis del software, hardware, comunicaciones, base de datos y casos de uso. Cada apartado detalla los componentes necesarios para garantizar la correcta implementación de la metodología, asegurando que la solución sea viable, escalable y alineada con los objetivos estratégicos de la organización.

Objetivos

Objetivo General

Elaborar una propuesta de metodología para el gestionamiento de la documentación en la nube basada en Microsoft OneDrive para la empresa Golden Comunicaciones S.A., apoyada en lineamientos de buenas prácticas internacionales como ISO 27001, ISO 9001 e ITIL, con el fin de mejorar la seguridad, control, acceso y administración de la información corporativa.

Objetivos Específicos

a. Crear controles de bloqueo que prevengan errores en archivos y carpetas.
b. Elaborar procedimientos que controlen los daños ocasionados por los usuarios.
c. Elaborar controles de seguridad para reducir los errores cometidos por los usuarios en el acceso a las carpetas.
d. Diseñar un plan de recuperación que permita el control de versiones de todos los documentos y archivos de la organización, garantizando que cada cambio quede registrado y que se pueda acceder a versiones anteriores en caso de pérdida o modificación no deseada.

Prevención de Conflictos de Edición y Bloqueo de Archivos

Errores de bloqueo en archivos y carpetas

Descripción del Problema

Los errores de bloqueo ocurren cuando varios usuarios intentan acceder y modificar simultáneamente un mismo archivo o carpeta, generando conflictos que restringen el acceso a otros usuarios.

Esta situación provoca:

a) Retrasos en los procesos administrativos.
b) Pérdida de productividad.
c) Riesgo de sobreescritura de información.
d) Confusión sobre la versión correcta del documento.
e) Dificultades en el trabajo colaborativo.

Descripción del Apartado Número Uno

Implementar una plataforma de colaboración en la nube, como Microsoft 365, con el fin de generar versionas guardadas en una línea del tiempo que permite restaurar cambios anteriores.

Guía De Desarrollo de la Investigación

"Propuesta de una metodología para el gestionamiento de la documentación en la nube para Golden Comunicaciones S.A."

Introducción

Actualmente, las organizaciones manejan grandes cantidades de información digital que requieren acceso rápido, seguro y colaborativo. En el caso de Microsoft 365, las plataformas en la nube permiten que múltiples usuarios trabajen simultáneamente sobre documentos compartidos, mejorando la productividad y la comunicación empresarial.

Sin embargo, en Golden Comunicaciones S.A. se presentan problemas relacionados con el bloqueo de archivos y carpetas, ocasionando conflictos de acceso, pérdida de tiempo y dificultades en la gestión documental. Por esta razón, se propone el diseño de una metodología de gestión documental basada en servicios de colaboración en la nube.

Justificación

La implementación de una metodología de gestión documental en la nube permite optimizar el manejo de archivos dentro de Golden Comunicaciones S.A., reduciendo los errores de bloqueo y mejorando la colaboración entre usuarios.

El uso de herramientas como Microsoft 365 permite:

a) Control de versiones.
b) Acceso simultáneo a documentos.
c) Restauración de cambios anteriores.
d) Seguridad de la información.
e) Disponibilidad remota de archivos.

Esto contribuirá a mejorar la eficiencia operativa y la continuidad de los procesos empresariales.

Objetivos

Objetivo General

Proponer una metodología para la gestión de documentación en la nube mediante el uso de Microsoft 365 en Golden Comunicaciones S.A., con el fin de disminuir los errores de bloqueo en archivos y carpetas.

Objetivos Específicos

a) Identificar las causas de los errores de bloqueo en archivos y carpetas.

b) Analizar el proceso actual de gestión documental de la empresa.

c) Diseñar una metodología de colaboración en la nube basada en Microsoft 365.

d) Establecer lineamientos para el control de versiones y acceso compartido.

e) Evaluar los beneficios de la implementación propuesta.

Marco Teórico

Gestión Documental

La gestión documental consiste en el conjunto de procesos utilizados para administrar documentos de manera eficiente durante todo su ciclo de vida.

Incluye

a) Creación.

b) Almacenamiento.

c) Organización.

d) Acceso.

e) Modificación.

f) Respaldo.

g) Eliminación.

Computación en la nube

La computación en la nube permite almacenar y administrar información mediante servidores remotos accesibles desde internet.

Beneficios

a) Acceso desde cualquier ubicación.

b) Respaldo automático.

c) Colaboración en tiempo real.

d) Mayor seguridad.

e) Escalabilidad.

Microsoft 365

Microsoft 365 es una plataforma de productividad y colaboración basada en la nube que integra herramientas como:

a) OneDrive.

b) SharePoint.

c) Teams.

d) Word.

e) Excel.

f) PowerPoint.

Funciones principales

a) Edición colaborativa.

b) Historial de versiones.

c) Sincronización automática.

d) Gestión de permisos.

- Recuperación de archivos.

Control de versiones

El control de versiones permite guardar diferentes estados de un documento a lo largo del tiempo.

Ventajas

a) Recuperar información eliminada.

b) Comparar cambios.

c) Evitar pérdida de datos.

d) Identificar modificaciones realizadas.

Diagnóstico de la Situación Actual

Actualmente la empresa presenta:

Tabla 4

Diagnóstico de la situación actual

Situaciones identificadas	**Consecuencia**
Uso compartido incorrecto de archivos.	Bloqueos constantes
Edición simultánea sin control	Conflictos de versiones
Falta de lineamientos documentales	Desorganización
Ausencia de respaldo automatizado	Riesgo de pérdida de información
Dependencia de almacenamiento local	Limitación de acceso
Uso compartido incorrecto de archivos	Bloqueos constantes

Nota. Elaboración propia, 2026.

Propuesta de Solución

Implementación de Microsoft 365

La propuesta consiste en implementar una plataforma colaborativa basada en Microsoft 365 para centralizar la documentación empresarial y mejorar el trabajo colaborativo.

Metodología Propuesta

La metodología propuesta se desarrolla en cinco fases secuenciales, las cuales permiten planificar, implementar y dar seguimiento a la solución tecnológica planteada.

Fase 1. Diagnóstico

Actividades

a) Identificar archivos con mayor incidencia de bloqueo.
b) Analizar el flujo documental.
c) Identificar usuarios involucrados.
d) Revisar permisos y accesos actuales.

Resultado esperado: Detección de los puntos críticos del sistema documental.

Fase 2. Diseño de la estructura documental

Actividades

a) Crear carpetas organizadas por departamentos.
b) Definir nomenclatura de archivos.
c) Establecer permisos de acceso.
d) Crear políticas de uso documental.

Resultado esperado: Estructura organizada y controlada.

Fase 3. Implementación de Microsoft 365

Herramientas utilizadas

a) OneDrive
b) SharePoint
c) Microsoft Teams

Actividades

a) Migración de documentos.
b) Configuración de permisos.
c) Activación del historial de versiones.
d) Sincronización de carpetas.
e) Configuración de acceso remoto.

Resultado esperado: Sistema documental colaborativo en la nube.

Fase 4. Capacitación

Temas de capacitación

a) Uso de OneDrive.
b) Edición colaborativa.
c) Recuperación de versiones.
d) Buenas prácticas documentales.
e) Gestión de permisos.

Resultado esperado: Usuarios capacitados para trabajar en la nube.

Fase 5. Seguimiento y control

Actividades

a) Monitorear bloqueos.
b) Evaluar accesos.
c) Revisar historial de cambios.
d) Aplicar mejoras continuas.

Resultado esperado: Reducción de errores y mejora continua.

Funcionamiento del Historial de Versiones

El historial de versiones permite guardar automáticamente cada modificación realizada en un documento.

Beneficios

a) Restaurar versiones anteriores.
b) Ver quién realizó cambios.
c) Recuperar información eliminada.
d) Evitar pérdida de documentos.

Beneficios Esperados

Tabla 5
Beneficios esperados de la implementación de Microsoft 365 en la gestión documental

Beneficio	**Impacto**
Reducción de bloqueos	Mayor productividad
Trabajo colaborativo	Mejor comunicación

Control de versiones	Seguridad documental
Acceso remoto	Mayor disponibilidad
Respaldo automático	Protección de información
Control de versiones	Seguridad documental

Nota. Elaboración propia, 2026.

Recursos Necesarios

Recursos tecnológicos

a) Licencias Microsoft 365.
b) Conexión a internet estable.
c) Equipos de cómputo actualizados.

Recursos humanos

a) Administrador TI.
b) Usuarios administrativos.
c) Equipo.

Cronograma de Actividades

Tabla 6

Cronograma de implementación de la propuesta metodológica

Actividad	Semana 1	Semana 2	Semana 3	Semana 4
Diagnóstico	X			
Diseño documental	X	X		
Implementación M365		X	X	
Capacitación			X	
Seguimiento				X

Nota. Elaboración propia, 2026.

Descripción del Apartado Número Dos

Configurar roles específicos para cada usuario, como editor, revisor o lector, ayuda a prevenir conflictos y a coordinar el trabajo colaborativo.

Configuración de Roles y Permisos de Usuario

Con el propósito de mejorar el control documental y reducir los conflictos de acceso en archivos y carpetas, se propone la configuración de roles específicos dentro de la plataforma colaborativa en la nube. La asignación de roles permite definir las acciones que cada usuario puede realizar sobre los documentos, fortaleciendo la organización y la seguridad de la información.

Roles propuestos

Tabla 7

Roles y permisos propuestos para la gestión documental

Rol	Función
Editor	Puede crear, modificar y actualizar documentos.
Revisor	Puede revisar archivos y realizar comentarios sin alterar el contenido principal.
Lector	Únicamente puede visualizar documentos sin realizar modificaciones.
Administrador	Gestiona permisos, accesos y configuraciones generales del sistema.

Nota. Elaboración propia, 2026.

Beneficios de la configuración de roles

La implementación de roles y permisos específicos proporciona los siguientes beneficios:

a) Prevención de conflictos por edición simultánea.

b) Mejor organización del trabajo colaborativo.

c) Mayor control sobre la documentación.

d) Reducción de modificaciones no autorizadas.

e) Incremento de la seguridad de la información.

Implementación en Microsoft 365

Mediante herramientas como SharePoint y OneDrive será posible asignar permisos específicos a cada usuario o grupo de trabajo, permitiendo administrar correctamente el acceso a los documentos empresariales.

Descripción del Apartado Número Tres

Automatizar el proceso de sincronización de archivos y carpetas en la nube.

Automatización del Proceso de Sincronización de Archivos y Carpetas en la nube

Otra necesidad identificada corresponde a la automatización de la sincronización de archivos y carpetas en la nube, con el propósito de garantizar que toda la información permanezca actualizada y disponible para los usuarios autorizados.

La sincronización automática permite que los cambios realizados en un documento se reflejen inmediatamente en todos los dispositivos conectados a la plataforma.

Objetivos de la automatización

a) Mantener actualizados los archivos en tiempo real.
b) Reducir errores manuales de almacenamiento.
c) Evitar pérdida de información.
d) Facilitar el acceso remoto a los documentos.
e) Garantizar disponibilidad continua de la información.

Funcionamiento propuesto

La sincronización se realiza mediante las herramientas integradas de Microsoft 365, lo que permite:

a) Carga automática de archivos.
b) Actualización inmediata de cambios.
c) Respaldo automático en la nube.
d) Acceso desde múltiples dispositivos.
e) Recuperación de archivos eliminados o modificados.

Beneficios Esperados

Tabla 8

Beneficios de la automatización de la sincronización de archivos y carpetas

Beneficio	Resultados esperados
Sincronización automática.	Información actualizada en tiempo real.
Respaldo constante.	Mayor seguridad documental.
Acceso remoto.	Disponibilidad desde cualquier ubicación
Menor intervención manual.	Reducción de errores humanos
Continuidad operativa	Mejor eficiencia empresarial

Nota. Elaboración propia, 2026.

Herramientas utilizadas

a) OneDrive.
b) SharePoint.
c) Microsoft Teams.

Estas herramientas permitirán centralizar la información y mantener la sincronización continua entre usuarios y departamentos de Golden Comunicaciones S.A.

Conclusiones

La implementación de una metodología de gestión documental en la nube mediante Microsoft 365 permite a Golden Comunicaciones S.A. reducir significativamente los errores de bloqueo en archivos y carpetas. Asimismo, la organización favorece la colaboración entre usuarios, optimiza el acceso a la información y garantiza un mejor control documental mediante herramientas de versionamiento y almacenamiento seguro.

Protección y Recuperación de la Información Documental

Daño en archivos y carpetas.

Descripción del Problema

Uno de los problemas principales identificados en Golden Comunicaciones S.A. corresponde al daño en archivos y carpetas dentro de la organización. Esta situación se presenta como consecuencia de diversos factores, entre ellos fallos de hardware, corrupción de datos, errores del sistema y acciones accidentales realizadas por los usuarios.

Como resultado, la empresa enfrenta pérdida de información crítica, retrasos en las actividades laborales y dificultades para recuperar documentos importantes. Además, la ausencia de un sistema automatizado de respaldo incrementa el riesgo de pérdida permanente de archivos, afectando la productividad y la seguridad documental de la organización.

Descripción del Apartado Número Uno

Implementar un sistema en la nube con respaldo automático, asegurando que los archivos se respalden continua y periódicamente.

Guía de implementación

"Propuesta de una metodología para el gestionamiento de la documentación en la nube para Golden Comunicaciones S.A."

Introducción

La gestión documental constituye un elemento fundamental dentro de las organizaciones, ya que permite administrar de manera eficiente la información utilizada en los procesos empresariales. En Golden Comunicaciones S.A. se ha identificado la necesidad de mejorar el manejo de archivos digitales debido a problemas relacionados con daños en documentos y carpetas. Estas situaciones afectan directamente la continuidad operativa y generan dificultades para acceder a información importante para la empresa. Por esta razón, se plantea la implementación de una metodología basada en servicios de almacenamiento y respaldo en la nube.

Necesidad identificada

La principal necesidad consiste en implementar un sistema de almacenamiento en la nube con respaldo automático que garantice la protección y el almacenamiento seguro de los archivos

empresariales. Este sistema debe realizar copias de seguridad de manera continua y periódica para garantizar la recuperación de la información ante cualquier incidente.

Asimismo, la solución permite mantener la disponibilidad de los documentos desde diferentes dispositivos y ubicaciones, favoreciendo el acceso oportuno a la información. La automatización de los respaldos reduce los riesgos derivados de errores humanos y fallos técnicos, fortaleciendo la gestión documental de Golden Comunicaciones S.A.

Objetivos

Objetivo General

Proponer una metodología para la implementación de un sistema de respaldo automático en la nube para Golden Comunicaciones S.A., con el propósito de reducir los daños y pérdidas de archivos y carpetas.

Objetivos Específicos

a) Identificar las causas que generan daños en archivos y carpetas.
b) Analizar el proceso actual de almacenamiento documental.
c) Diseñar una metodología de respaldo automático en la nube.
d) Implementar herramientas de sincronización y recuperación de archivos.
e) Mejorar la seguridad y disponibilidad de la información empresarial**.**

Justificación

La implementación de un sistema de respaldo automático en la nube permitirá a Golden Comunicaciones S.A. fortalecer la protección de su información empresarial. En la actualidad, la organización enfrenta riesgos asociados a la pérdida de archivos ocasionada por daños físicos, errores humanos y problemas tecnológicos.

Mediante el uso de plataformas colaborativas en la nube, será posible mantener copias de seguridad actualizadas y accesibles en todo momento. Además, esta propuesta contribuye a optimizar la continuidad operativa, reducir tiempos de recuperación y garantizar una mayor seguridad documental dentro de la empresa.

Marco teórico

Gestión documental

La gestión documental comprende el conjunto de procesos orientados al control y administración de documentos dentro de una organización. Su objetivo principal es garantizar que la información sea almacenada, organizada y recuperada de manera eficiente. Una adecuada gestión documental facilita el acceso rápido a los archivos y disminuye los riesgos de pérdida de información. Además, contribuye al cumplimiento de políticas internas relacionadas con la seguridad y confidencialidad de los datos empresariales**.**

Computación en la nube

La computación en la nube consiste en el uso de servidores remotos accesibles mediante internet para almacenar y procesar información. Este modelo tecnológico permite que los usuarios accedan a sus archivos desde diferentes dispositivos y ubicaciones sin depender exclusivamente de almacenamiento físico local. Entre sus principales beneficios destacan la escalabilidad, disponibilidad continua, respaldo automático y colaboración en tiempo real. Actualmente, las soluciones en la nube son ampliamente utilizadas por organizaciones que buscan optimizar la administración de información digital.

Respaldo automático de información

El respaldo automático es un proceso mediante el cual los archivos se copian y almacenan periódicamente en un entorno seguro sin necesidad de intervención manual constante. Este mecanismo permite recuperar documentos en caso de daños, eliminación accidental o fallos del sistema. La automatización de copias de seguridad reduce significativamente el riesgo de pérdida permanente de información. Además, facilita la continuidad operativa de las organizaciones al garantizar la disponibilidad constante de los archivos empresariales.

Herramientas tecnológicas propuestas

Para la implementación de la metodología se propone utilizar herramientas de Microsoft 365, debido a sus capacidades de almacenamiento, sincronización y respaldo documental en la nube.

Herramientas principales

a. OneDrive.

b. SharePoint.
c. Microsoft Teams.

Estas plataformas permitirán centralizar la documentación empresarial y automatizar los procesos de respaldo y recuperación de información.

Metodología de Implementación

Fase 1. Diagnóstico inicial

En esta fase se realiza un análisis detallado de la situación actual de la empresa en relación con el manejo de archivos y carpetas. Se identifican los documentos críticos, los dispositivos utilizados y las principales causas de daño o pérdida de información. Asimismo, se revisan los métodos actuales de almacenamiento y respaldo implementados dentro de la organización. Esta evaluación permitirá establecer las necesidades técnicas y operativas requeridas para la implementación del sistema en la nube**.**

Fase 2. Diseño de la estructura documental

Durante esta etapa se define la organización de carpetas y archivos dentro de la plataforma en la nube. Se establecen categorías documentales, permisos de acceso y políticas de almacenamiento para cada departamento de la empresa. Además, se diseñan lineamientos relacionados con nombres de archivos y control documental. Una correcta estructura facilitará la administración de la información y permitirá mantener un entorno organizado y seguro para todos los usuarios.

Fase 3. Implementación del sistema de respaldo automático

Esta fase consiste en configurar las herramientas de almacenamiento en la nube para realizar respaldos automáticos y sincronización continua de archivos. Se habilitarán funciones de copia de seguridad periódica y recuperación de versiones anteriores de documentos. Asimismo, se configura el acceso desde múltiples dispositivos para garantizar la disponibilidad permanente de la información. Este proceso protege los archivos empresariales frente a daños, corrupción de datos o eliminación accidental.

Fase 4. Configuración de sincronización en la nube

En esta fase se activa la sincronización automática entre equipos locales y la plataforma en la nube. Cada modificación realizada en los documentos será actualizada automáticamente dentro del sistema, evitando inconsistencias entre versiones de archivos. La sincronización en tiempo real facilitará el trabajo colaborativo y reducirá los riesgos asociados a pérdidas de información.

Además, permite que los usuarios accedan a documentos actualizados desde cualquier ubicación autorizada.

Fase 5. Capacitación de usuarios

La capacitación tiene como finalidad enseñar a los colaboradores el uso correcto de las herramientas implementadas. Se brindará formación sobre almacenamiento en la nube, recuperación de archivos, sincronización automática y buenas prácticas de seguridad documental. Asimismo, los usuarios aprenden a identificar posibles riesgos relacionados con el manejo inadecuado de información. Una capacitación adecuada contribuye a reducir errores humanos y garantizar el aprovechamiento eficiente de la plataforma.

Fase 6. Seguimiento y control

Después de la implementación, se realizará un monitoreo constante del funcionamiento del sistema de respaldo automático. Se verifican los procesos de sincronización, disponibilidad de archivos y efectividad de las copias de seguridad realizadas. Además, se evalúa el desempeño de la plataforma y se aplicarán mejoras continuas según las necesidades de la empresa. Esta fase permitirá asegurar la estabilidad del sistema y mantener la protección permanente de la información empresarial.

Beneficios Esperados

Tabla 9

Beneficios esperados de la implementación del sistema de respaldo automático

Beneficio	Resultado esperado
Respaldo automático.	Protección continua de archivos.
Recuperación de documentos.	Menor pérdida de información.
Sincronización en tiempo real.	Actualización constante
Acceso remoto	Disponibilidad desde cualquier lugar
Seguridad documental	Mayor protección de datos
Reducción de errores humanos	Mejor control operativo

Nota. Elaboración propia, 2026.

Recursos Necesarios

Recursos tecnológicos

a) Licencias de Microsoft 365.
b) Equipos de cómputo actualizados.
c) Acceso estable a internet.
d) Servidores y almacenamiento en la nube.

Recursos humanos

a) Personal de soporte técnico.
b) Administrador de sistemas.
c) Usuarios administrativos y operativos.

Cronograma de Actividades

Tabla 10

Cronograma de actividades para la implementación de la metodología

Actividad	Semana 1	Semana 2	Semana 3
Diagnóstico inicial	**X**		
Diseño documental	**X**	**X**	
Implementación del sistema		**X**	**X**
Configuración de sincronización			**X**
Capacitación			**X**
Seguimiento y control			**X**

Nota. Elaboración propia, 2026.

Conclusiones

La implementación de una metodología de gestión documental basada en servicios de respaldo automático en la nube permitirá a Golden Comunicaciones S.A. reducir significativamente los riesgos asociados al daño y pérdida de archivos. La automatización de copias de seguridad garantizará la disponibilidad permanente de la información y facilitará la recuperación de documentos ante cualquier incidente.

Además, el uso de plataformas colaborativas contribuirá a optimizar los procesos internos y mejora la seguridad documental mediante mecanismos de respaldo, sincronización y recuperación de la información.

Descripción del Apartado Número Dos

Se desarrollará una normativa para la revisión de versiones en archivos, proporciona una forma rápida de restaurar la información perdida.

Normativa para la Revisión y Control de Versiones en Archivos

Introducción

La presente normativa tiene como finalidad establecer lineamientos para la revisión y control de versiones de archivos dentro de Golden Comunicaciones S.A. Su propósito es garantizar

la protección de la información empresarial mediante mecanismos que permitan recuperar documentos modificados, dañados o eliminados accidentalmente.

Asimismo, esta normativa permitirá mantener un historial organizado de modificaciones realizadas sobre los archivos almacenados en la nube. La implementación de controles de versiones fortalece la seguridad documental, la trazabilidad de cambios y la continuidad operativa de la organización.

Objetivo de la Normativa

El objetivo principal de esta normativa es regular el proceso de revisión y control de versiones de archivos digitales almacenados en la nube. Asimismo, busca proporcionar un mecanismo ágil y eficiente para restaurar información perdida o afectada por errores humanos, daños en documentos o modificaciones incorrectas.

Mediante el establecimiento de políticas de control documental, la empresa podrá asegurar que cada archivo mantenga un historial de cambios organizado y accesible. De esta manera, se fortalece la gestión documental y se reducen los riesgos asociados a la pérdida de información crítica.

Alcance

La normativa aplica a todos los colaboradores de Golden Comunicaciones S.A. que tengan acceso a archivos y carpetas almacenadas en la plataforma de gestión en la nube.

Comprende los documentos administrativos, financieros, operativos y cualquier otro archivo digital utilizado dentro de la organización. Asimismo, es de cumplimiento obligatorio para usuarios con permisos de edición, revisión y administración documental.

Su aplicación garantiza un manejo adecuado de la información y preserva la integridad, disponibilidad y trazabilidad de los documentos empresariales.

Políticas de Control de Versiones

Registro automático de versiones

Todos los documentos almacenados en la plataforma de Microsoft 365 deberán mantener habilitado el historial de versiones. Cada modificación realizada sobre un archivo genera automáticamente una nueva versión almacenada en el sistema.

Este procedimiento conserva un registro cronológico de cambios y facilitará la recuperación de información cuando sea necesario e identifica el usuario responsable de cada modificación y la fecha en que se realiza.

Revisión periódica de documentos

Los responsables de cada área deberán realizar revisiones periódicas de los documentos almacenados en la nube con el fin de verificar la integridad y actualización de la información.

Estas revisiones permiten detectar posibles errores, archivos duplicados o modificaciones incorrectas. Asimismo, contribuyen a mantener organizada la documentación empresarial y evitar problemas relacionados con versiones desactualizadas. La revisión constante garantizará un mejor control documental dentro de la organización.

Restauración de Versiones Anteriores

En caso de pérdida de información, modificación incorrecta o corrupción de archivos, los usuarios autorizados podrán restaurar versiones anteriores de los documentos almacenados en la nube.

Este procedimiento permite recuperar rápidamente información afectada sin necesidad de reconstruir el archivo manualmente, reduciendo con ello, tiempos de recuperación y minimizando los impactos operativos ocasionados por incidentes documentales. Además, proporcionará mayor seguridad y confiabilidad en el manejo de archivos empresariales.

Roles y Responsabilidades

Tabla 11

Roles y responsabilidades para el control de versiones

Rol	**Responsabilidad**
Administrador del sistema	Supervisar el control de versiones y permisos de acceso.
Editor	Modificar y actualizar documentos autorizados
Revisor	Verificar cambios y validar información documental.
Usuario lector	Consultar documentos sin realizar modificaciones.
Soporte técnico	Gestionar recuperación de archivos y respaldos.

Nota. Elaboración propia, 2026.

Procedimiento para el Control de Versiones

Paso 1. Creación del archivo

El usuario autorizado crea el documento dentro de la plataforma en la nube utilizando las herramientas definidas por la organización.

Paso 2. Modificación del documento

Cada vez que un archivo sea editado, el sistema generará automáticamente una nueva versión dentro del historial documental.

Paso 3. Validación de cambios

Los revisores verifican que las modificaciones realizadas sean correctas y estén alineadas con las políticas documentales de la empresa.

Paso 4. Almacenamiento automático

El sistema almacenará cada versión del documento de manera segura dentro de la nube, garantizando respaldo continuo.

Paso 5. Restauración de versiones

En caso de errores o pérdida de información, el usuario autorizado podrá acceder al historial y restaurar una versión anterior del archivo.

Herramientas Tecnológicas Utilizadas

La implementación de la normativa se apoya en herramientas de Microsoft 365, las cuales permiten administrar el historial de versiones y la recuperación de archivos.

Herramientas principales

a) OneDrive.
b) SharePoint.
c) Microsoft Teams.

Estas plataformas facilitarán el almacenamiento seguro, la sincronización automática y el control de cambios sobre los documentos empresariales.

Beneficios de la Normativa

Tabla 12

Beneficios de la implementación de la normativa para el control de versiones

Beneficio	Resultado esperado
Historial de versiones.	Mayor control documental
Restauración rápida	Recuperación eficiente de archivos
Registro de cambios	Trazabilidad de modificaciones
Seguridad documental	Protección de información crítica
Reducción de errores	Menor pérdida de información
Organización documental	Mejor administración de archivos

Nota. Elaboración propia, 2026.

Seguimiento y Control de la Normativa

El cumplimiento de la normativa será supervisado periódicamente por el área de tecnología y administración documental de Golden Comunicaciones S.A. Se realiza auditorías internas para verificar que los usuarios mantengan habilitado el control de versiones y utilicen correctamente las herramientas de almacenamiento en la nube. Asimismo, se evaluará la efectividad de los procedimientos de restauración y recuperación de archivos. El seguimiento continuo permitirá identificar oportunidades de mejora y garantizar el correcto funcionamiento del sistema documental.

Conclusión

La implementación de una normativa para la revisión y control de versiones en archivos permitirá fortalecer la gestión documental dentro de Golden Comunicaciones S.A. El establecimiento de políticas claras facilitará la recuperación rápida de información perdida y mejorará la organización de documentos almacenados en la nube.

Además, la incorporación del historial de versiones contribuirá a reducir riesgos asociados a daños, errores humanos y modificaciones incorrectas. Esta propuesta permitirá garantizar una mayor seguridad, disponibilidad y confiabilidad de la información empresarial.

Fortalecimiento de la Seguridad y el Control de Accesos a la Documentación

Alteración de permisos a los usuarios por externos.

Descripción del Problema

Actualmente, la organización no cuenta con controles de seguridad que impidan que usuarios externos manipulen o dañen los permisos de acceso en carpetas alojadas en la nube. Esta situación puede provocar bloqueos de acceso y afectaciones en la disponibilidad e integridad de la información.

Descripción de Apartado Número Uno

Integrar los controles de seguridad mediante un cuadro comparativo que identifique las acciones que se desea implementar y su relación con los controles establecidos en la ISO 27001, con el propósito de fortalecer la gestión de la seguridad de la información.

Objetivo de los Controles de Seguridad

Implementar controles de seguridad basados en la norma internacional ISO 27001 - Gestión de la Seguridad de la Información, con el fin de proteger los permisos de acceso, garantizar la integridad documental y evitar modificaciones no autorizadas por usuarios externos.

Tabla 13

Cuadro Comparativo de Controles de Seguridad Basados en ISO 27001

Acción que se desea realizar	Riesgo identificado	Control de Seguridad Propuesto	Relación con ISO 27001	Descripción detallada del control
Restringir modificaciones de permisos en carpetas	Usuarios externos modifican permisos de acceso	Implementación de control de acceso basado en roles (RBAC)	Control de Acceso – ISO 27001 *(Véase Anexo A)*	Se asignarán permisos según funciones específicas dentro de la organización. Solo administradores autorizados podrán modificar permisos de carpetas y archivos
Evitar accesos no autorizados	Ingreso de usuarios externos a carpetas críticas	Autenticación multifactorial (MFA)	Seguridad de Acceso	Todo usuario deberá validar su identidad mediante contraseña y código adicional desde dispositivo móvil o correo autorizado.
Detectar cambios indebidos en permisos	Alteraciones sin conocimiento del administrador	Auditoría y registro de eventos	Gestión de Logs y Monitoreo	El sistema registrará cada cambio realizado en permisos, identificando usuario, fecha, hora y acción ejecutada.
Proteger carpetas críticas del servidor	Manipulación o eliminación accidental o maliciosa	Segmentación y clasificación de información	Clasificación de Activos	Las carpetas serán clasificadas según nivel de sensibilidad: pública, interna, confidencial y restringida.
Controlar acceso de terceros	Proveedores externos con privilegios excesivos	Política de acceso para terceros	Gestión de Relaciones con Proveedores	Los accesos externos serán temporales, limitados y monitoreados continuamente.
Restaurar permisos afectados	Pérdida de acceso a carpetas	Copias de seguridad de configuraciones y permisos	Continuidad del Negocio	Se realizará respaldo automático de configuraciones y permisos para restaurarlos rápidamente ante incidentes.

Acción que se desea realizar	Riesgo identificado	Control de Seguridad Propuesto	Relación con ISO 27001	Descripción detallada del control
Limitar privilegios administrativos	Uso indebido de cuentas con privilegios altos	Principio de mínimo privilegio	Gestión de Identidades y Accesos	Cada usuario tendrá únicamente los permisos necesarios para realizar sus funciones laborales.
Prevenir ataques por robo de credenciales	Acceso ilícito mediante contraseñas vulneradas	Políticas robustas de contraseñas	Seguridad de Autenticación	Se implementarán contraseñas complejas, expiración periódica y bloqueo por intentos fallidos.
Supervisar actividades sospechosas	Actividades anormales en la nube	Monitoreo continuo de seguridad	Gestión de Incidentes	Se utilizarán alertas automáticas ante cambios sospechosos de permisos o accesos fuera de horario.
Evitar propagación de daños	Modificación masiva de carpetas	Separación de ambientes y permisos	Seguridad Operacional	Se dividirán ambientes administrativos, operativos y de usuarios finales para reducir riesgos.
Evitar propagación de daños	Modificación masiva de carpetas	Separación de ambientes y permisos	Seguridad Operacional	Se dividirán ambientes administrativos, operativos y de usuarios finales para reducir riesgos.
Garantizar trazabilidad	Desconocimiento de responsables de cambios	Bitácora de actividades	Registro y Evidencia	Se almacenará historial detallado de accesos, modificaciones y eliminaciones realizadas.
Reducir errores humanos	Usuarios modifican permisos incorrectamente	Capacitación en seguridad documental	Concientización en Seguridad	El personal recibirá formación periódica sobre manejo seguro de documentos y permisos.

Acción que se desea realizar	Riesgo identificado	Control de Seguridad Propuesto	Relación con ISO 27001	Descripción detallada del control
Validar autorizaciones antes de cambios	Cambios realizados sin aprobación	Flujo de aprobación para modificaciones	Gestión de Cambios	Toda modificación de permisos deberá ser autorizada por el administrador o encargado TI.
Proteger sesiones activas	Secuestro de sesiones en la nube	Cierre automático de sesiones	Seguridad de Sesiones	El sistema cerrará sesiones inactivas automáticamente después de un tiempo definido.
Garantizar disponibilidad de documentos	Bloqueo de acceso por manipulación externa	Plan de recuperación ante incidentes	Continuidad y Recuperación	Se establecerán procedimientos para restaurar accesos y recuperar operaciones rápidamente.
Evitar propagación de daños	Modificación masiva de carpetas	Separación de ambientes y permisos	Seguridad Operacional	Se dividirán ambientes administrativos, operativos y de usuarios finales para reducir riesgos.
Garantizar trazabilidad	Desconocimiento de responsables de cambios	Bitácora de actividades	Registro y Evidencia	Se almacenará historial detallado de accesos, modificaciones y eliminaciones realizadas.
Reducir errores humanos	Usuarios modifican permisos incorrectamente	Capacitación en seguridad documental	Concientización en Seguridad	El personal recibirá formación periódica sobre manejo seguro de documentos y permisos.
Validar autorizaciones antes de cambios	Cambios realizados sin aprobación	Flujo de aprobación para modificaciones	Gestión de Cambios	Toda modificación de permisos deberá ser autorizada por el administrador o encargado TI.

Nota. Elaboración propia, 2026.

Desarrollo Detallado de los Controles de Seguridad

Control de Acceso Basado en Roles

Descripción

Consiste en asignar permisos según el puesto o función del usuario dentro de la organización.

Implementación

a) Crear perfiles de usuario:
b) Administrador
c) Supervisor
d) Usuario estándar
e) Usuario externo
f) Restringir modificación de permisos únicamente a administradores.
g) Separar permisos de lectura, escritura y eliminación.

Beneficios

a) Reduce accesos indebidos.
b) Evita modificaciones accidentales.
c) Mejora el control organizacional.

Implementación de Autenticación Multifactor

Descripción

Sistema de doble validación para acceder a la nube.

Implementación

a) Contraseña + código temporal.
b) Uso de aplicaciones autenticadoras.
c) Validación por correo corporativo.

Beneficios

a) Evita accesos con credenciales robadas.
b) Incrementa la protección de cuentas administrativas.

Auditoría y Monitoreo de Eventos

Descripción

Registro detallado de actividades realizadas sobre carpetas y permisos.

Implementación

a) Activar logs del servidor.
b) Registrar:
    a. Usuario.
    b. Fecha.
    c. Dirección IP.
    d. Cambio realizado
c) ·Configurar alertas automáticas.

Beneficios

a) Permite identificar responsables.
b) Facilita investigaciones de incidentes.

Política de Mínimo Privilegio

Descripción

Los usuarios solo tendrán acceso a lo estrictamente necesario.

Implementación

a) Revisiones mensuales de permisos.
b) Eliminación de privilegios innecesarios.
c) Control de cuentas inactivas.

Beneficios

a) Reduce riesgos internos y externos.
b) Limita el impacto de ataques.

Copias de Seguridad de Permisos y Configuraciones

Descripción

Respaldo automático de configuraciones críticas.

Implementación

a) Backups diarios.
b) Almacenamiento seguro.
c) Restauración rápida de permisos.

Beneficios

a) Recuperación rápida ante errores.
b) Continuidad operativa.

Capacitación y Concientización

Descripción

Entrenamiento del personal sobre riesgos de seguridad documental.

***I*mplementación**

a) Charlas trimestrales.
b) Simulaciones de incidentes.
c) Manuales de buenas prácticas.

Beneficios

Reduce errores humanos.

Mejora cultura organizacional.

Propuesta de Metodología de Implementación

Tabla 14

Metodología para la implementación de controles de seguridad basados en la norma ISO/IEC 27001

Fase	Actividad	Resultado Esperado
Diagnóstico	Identificar vulnerabilidades actuales	Detección de riesgos
Diseño	Definir controles basados en ISO 27001	Plan de seguridad
Implementación	Aplicar controles técnicos y administrativos	Protección documental
Monitoreo	Supervisar accesos y cambios	Detección temprana

Mejora continua	Actualizar políticas y controles	Optimización permanente

Nota. Elaboración propia, 2026

La implementación de controles de seguridad basados en ISO/ IEC 27001 permite fortalecer la protección documental en la nube de Golden Comunicaciones S.A., evitando la manipulación no autorizada de permisos por usuarios externos. Asimismo, favorece la confidencialidad, integridad y disponibilidad de la información, reduciendo riesgos operativos y mejorando la continuidad del negocio.

Descripción de Apartado Número Dos

Se desarrolla un plan para la revisión y el control de cambios en archivos y carpetas, con el objetivo de proteger la información que manipule cada usuario y persona externa.

"Plan de Revisión y Control de Cambios en Archivos y Carpetas para la Protección de la Información en la Nube".

Objetivo General

Establecer un procedimiento de revisión, monitoreo y control de los cambios realizados en archivos, carpetas y permisos de acceso dentro de la plataforma de almacenamiento en la nube, con el propósito de proteger la confidencialidad, integridad y disponibilidad de la información, minimizando el riesgo de alteraciones no autorizadas por usuarios internos o externos.

Objetivos Específicos

a) Identificar cambios realizados en archivos y carpetas.
b) Verificar modificaciones en permisos de acceso.
c) Detectar actividades sospechosas o no autorizadas.
d) Mantener trazabilidad de las acciones realizadas por los usuarios.
e) Garantizar la recuperación de información ante incidentes.
f) Cumplir con los lineamientos de seguridad establecidos por la organización.

Alcance

Este plan aplica a:

a) Usuarios internos.
b) Usuarios externos autorizados.

c) Administradores de sistemas.
d) Carpetas compartidas.
e) Documentos almacenados en la nube.
f) Configuración de permisos y accesos.

Responsables

Tabla 15

Responsables del Plan de Revisión y Control de Cambios

Responsable	**Función**
Administrador de TI	Supervisar y aprobar cambios de permisos
Encargado de Seguridad de la Información	Revisar auditorías y controles
Jefaturas de Área	Autorizar accesos a información sensible
Usuarios Finales	Reportar actividades sospechosas
Proveedores Externos	Cumplir las políticas de acceso establecidas

Nota. Elaboración propia, 2026

Procedimiento de Revisión de Cambios

Actividad 1. Monitoreo de Cambios

Descripción

Se realiza un monitoreo continuo de todas las acciones ejecutadas sobre los archivos, las carpetas y los permisos almacenados en la plataforma de gestión documental en la nube. Este control permitirá identificar quién realizó una modificación, cuándo se efectuó y qué elementos fueron afectados. Asimismo, se registran las actividades como creación, edición, eliminación y compartición de documentos, así como cambios en los permisos de acceso.

La información recopilada será utilizada para detectar comportamientos inusuales, prevenir incidentes de seguridad y mantener la trazabilidad de las operaciones realizadas por usuarios internos y externos. Los registros generados deberán almacenarse de forma segura para futuras auditorías e investigaciones.

Información para registrar

a) Nombre del usuario.
b) Fecha y hora.
c) Dirección IP.
d) Archivo o carpeta modificada.
e) Tipo de acción realizada:
    a. Creación.
    b. Edición.
    c. Eliminación.
    d. Cambio de permisos.
    e. Compartición externa.

Frecuencia: Monitoreo continuo.

Actividad 2. Revisión de Permisos

Descripción

La revisión de permisos consiste en verificar periódicamente que los accesos asignados a usuarios, grupos y terceros continúen siendo necesarios para el desempeño de sus funciones. Durante esta revisión se identificarán privilegios excesivos, cuentas inactivas y permisos otorgados sin autorización formal. También se validará que los accesos a información sensible estén restringidos únicamente al personal autorizado.

Esta actividad busca aplicar el principio de mínimo privilegio, reduciendo el riesgo de modificaciones indebidas o accesos no autorizados. Los resultados de cada revisión deberán documentarse y las correcciones encontradas deberán aplicarse de manera inmediata para fortalecer la seguridad de la información.

Actividades

a) Revisar usuarios activos.
b) Identificar permisos excesivos.
c) Eliminar accesos innecesarios.
d) Validar accesos de terceros.

Frecuencia: Mensual.

Actividad 3. Revisión del Historial de Versiones

Descripción

Se lleva a cabo una revisión periódica del historial de versiones de los documentos considerados críticos para la organización. El objetivo es verificar los cambios realizados por los usuarios, identificar modificaciones no autorizadas y garantizar la integridad de la información almacenada.

Esta actividad permite comparar versiones anteriores con las actuales para determinar la naturaleza de los cambios efectuados y validar que responde a necesidades operativas legítimas.

En caso de detectar errores o alteraciones indebidas, se podrá restaurar una versión previa del documento. Asimismo, el historial de versiones servirá como evidencia para auditorías y procesos de investigación relacionados con incidentes de seguridad.

Actividades

a) Revisar versiones modificadas.
b) Comparar cambios realizados.
c) Identificar modificaciones no autorizadas.
d) Restaurar versiones anteriores cuando sea necesario.

Frecuencia: Semanal.

Actividad 4. Auditoría de Accesos Externos

Descripción

Se realiza una auditoría periódica de los accesos otorgados a usuarios externos, proveedores o colaboradores temporales que interactúan con la documentación en la nube. Durante este proceso se verificará que cada acceso tenga una justificación válida, una autorización formal y una fecha de vencimiento definida. Además, se analizarán las actividades realizadas por estos usuarios para identificar comportamientos anómalos o acciones que puedan comprometer la seguridad de la información.

Los accesos que ya no sean necesarios serán eliminados de forma inmediata para reducir riesgos. Esta medida contribuye a mantener un control efectivo sobre terceros y a proteger los activos de información de la organización.

Actividades

a) Verificar accesos concedidos.
b) Revisar fechas de vencimiento.
c) Confirmar necesidad del acceso.
d) Eliminar accesos finalizados.

Frecuencia: Quincenal.

Actividad 5. Validación de Carpetas Críticas

Descripción

La validación de carpetas críticas tiene como propósito revisar periódicamente aquellas ubicaciones que contienen información sensible, confidencial o estratégica para la organización. Se verificará que los permisos asignados sean correctos, que los propietarios de las carpetas estén debidamente identificados y que no existan accesos no autorizados.

Asimismo, se revisa la configuración de compartición y las herencias de permisos que puedan representar vulnerabilidades de seguridad.

Esta actividad permite detectar configuraciones incorrectas que faciliten la manipulación o eliminación de información por parte de usuarios no autorizados. Los hallazgos encontrados deberán documentarse y corregirse oportunamente para garantizar la protección de los activos documentales.

Actividades

a) Revisar propietarios.
b) Revisar permisos heredados.
c) Verificar configuraciones de seguridad.
d) Comprobar accesos compartidos.

Frecuencia: Mensual.

Controles de Seguridad Propuestos

Tabla 16

Controles de Seguridad Propuestos para la Revisión y Control de Cambios

Control	Descripción	Beneficio
Registro de auditoría.	Almacena todas las acciones realizadas.	Trazabilidad.
Control de versiones.	Guarda versiones anteriores de documentos.	Recuperación rápida.
Autenticación multifactor.	Solicita doble validación de acceso.	Prevención de accesos indebidos.
Principio de mínimo privilegio.	Asigna únicamente los permisos necesarios.	Reducción de riesgos.
Alertas automáticas.	Notifica cambios sospechosos	Detección temprana.
Copias de seguridad.	Respaldo de información y permisos.	Recuperación ante incidentes.
Revisión periódica de accesos.	Validación continua de permisos.	Eliminación de privilegios innecesarios.

Nota. Elaboración propia, 2026

Indicadores de Seguimiento

Tabla 17

Indicadores para el Seguimiento del Plan

Indicador	Fórmula	Meta
Cambios revisados	Cambios revisados / Cambios registrados × 100	100%
Permisos auditados	Permisos auditados / Permisos existentes × 100	100%
Incidentes detectados	Total, de incidentes identificados	Tendencia decreciente
Recuperación de información	Incidentes recuperados / Incidentes reportados × 100	95% o más
Accesos externos revisados	Accesos revisados / Accesos otorgados × 100	100%

Nota. Elaboración propia, 2026

Plan de Acción ante Incidentes

Tabla 18

Plan de Acción ante Incidentes de Seguridad

Situación Detectada	Acción Correctiva
Cambio no autorizado de permisos	Restaurar permisos y bloquear usuario
Eliminación accidental de archivos	Recuperar versión anterior o respaldo
Acceso externo sospechoso	Suspender acceso y realizar investigación
Modificación indebida de documentos	Restaurar versión válida y documentar incidente
Compartición no autorizada	Revocar acceso y notificar a Seguridad de la Información

Nota. Elaboración propia, 2026

La implementación de este plan permitirá mantener un control permanente sobre los cambios realizados en archivos, carpetas y permisos de acceso, garantizando que toda modificación quede registrada, sea revisada y pueda revertirse en caso de incidentes. Además, fortalecerá la protección de la información frente a accesos indebidos y manipulaciones realizadas por usuarios externos, asegurando la continuidad y seguridad de la documentación almacenada en la nube.

Descripción de Apartado Número Tres

Se desarrolla una revisión para verificar los permisos existentes en cada usuario y/o persona externa que tenga acceso confiable y de esta manera una limpieza en caso de que las personas no tengan acceso porque ya no laboren en la compañía.

Plan de Verificación de Permisos y Depuración de Accesos

Objetivo

Verificar periódicamente los permisos asignados a usuarios internos y externos que acceden a la documentación almacenada en la nube, con el fin de identificar accesos innecesarios, cuentas inactivas o usuarios que ya no mantienen una relación laboral o contractual con la organización, reduciendo así los riesgos de alteración de permisos, pérdida de información y accesos no autorizados.

Alcance

Este procedimiento aplica a:

a) Usuarios internos.

b) Usuarios externos.

c) Proveedores.

d) Consultores.

e) Cuentas administrativas.

f) Carpetas compartidas.

g) Documentos críticos almacenados en la nube.

Procedimiento de Verificación de Permisos

Actividad 1. Inventario de Usuarios con Acceso

Descripción

Se realiza un levantamiento completo de todos los usuarios que poseen acceso a la plataforma documental en la nube. Durante esta actividad se identificará el nombre del usuario, área de trabajo, tipo de acceso asignado y recursos a los que puede ingresar. El inventario deberá incluir tanto personal interno como usuarios externos autorizados. La información recopilada permitirá conocer el estado actual de los accesos existentes y servirá como base para las revisiones posteriores. Además, se verifica que cada cuenta esté asociada a una persona responsable y debidamente identificada dentro de la organización.

Frecuencia: Mensual.

Actividad 2. Verificación de Vigencia de Usuarios

Descripción

Se revisará que todos los usuarios registrados continúen manteniendo una relación laboral, contractual o de servicio con la organización. Para ello se coordinará con el departamento de Recursos Humanos y las jefaturas correspondientes para validar la permanencia de cada usuario. En caso de detectar colaboradores que ya no laboran en la empresa o proveedores cuyos contratos hayan finalizado, se procederá a documentar la situación y gestionar la eliminación de sus accesos. Esta actividad busca evitar que cuentas obsoletas permanezcan activas y representen una vulnerabilidad para la seguridad de la información.

Frecuencia: Mensual.

Actividad 3. Revisión de Permisos Asignados

Descripción

Se verificará que los permisos otorgados a cada usuario correspondan a las funciones que desempeña dentro de la organización. Durante la revisión se identificarán permisos excesivos, accesos heredados y privilegios que ya no sean necesarios para la ejecución de las actividades laborales. Asimismo, se validará que los usuarios externos únicamente tengan acceso a la información requerida para cumplir con sus responsabilidades específicas. Los permisos que excedan las necesidades operativas serán ajustados o eliminados para cumplir con el principio de mínimo privilegio y reducir riesgos de seguridad.

Frecuencia: Mensual.

Actividad 4. Depuración de Usuarios Inactivos

Descripción:

Se llevará a cabo una revisión de las cuentas que no hayan presentado actividad durante un período previamente definido por la organización. Estas cuentas serán evaluadas para determinar si continúan siendo necesarias o si deben ser deshabilitadas. La depuración incluirá usuarios internos, externos y cuentas temporales creadas para proyectos específicos. Esta actividad permite reducir la superficie de exposición a amenazas y evitar que credenciales olvidadas puedan ser utilizadas de manera indebida por terceros. Toda eliminación o desactivación deberá quedar documentada como evidencia del control realizado.

Frecuencia: Trimestral.

Actividad 5. Eliminación y Corrección de Accesos No Autorizados

Descripción

Una vez identificados usuarios sin autorización vigente o permisos asignados incorrectamente, se procederá a la eliminación o corrección de dichos accesos. El administrador responsable documentará los cambios realizados, indicando la fecha, motivo y usuario afectado. Asimismo, se verificará que la revocación del acceso no genere afectaciones operativas para la organización. Este control busca garantizar que únicamente las personas autorizadas mantengan acceso a la documentación y que los permisos se encuentren alineados con las políticas de seguridad establecidas por la empresa.

Frecuencia: Inmediata después de cada revisión.

Matriz de Verificación de Usuarios y Permisos

Tabla 19

Matriz de verificación de usuarios y permisos

Usuario	**Área**	**Tipo de Usuario**	**Permiso Actual**	**¿Sigue Laborando?**	**¿Permiso Justificado?**	**Acción Requerida**
Usuario A	Administración	Interno	Administrador	Sí	Sí	Mantener
Usuario B	Ventas	Interno	Edición	No	No	Eliminar acceso
Usuario C	Proveedor	Externo	Lectura	Contrato vencido	No	Revocar acceso
Usuario D	Finanzas	Interno	Control Total	Sí	No	Ajustar permisos

Nota. Elaboración propia, 2026

Mediante la implementación de este plan se espera mantener un control actualizado de los accesos a la documentación en la nube, eliminando cuentas obsoletas, usuarios que ya no laboran en la organización y permisos innecesarios. Esto permitirá disminuir significativamente el riesgo de alteración de permisos por parte de usuarios externos, fortalecer la seguridad de la información y garantizar que únicamente las personas autorizadas tengan acceso a los recursos documentales de la empresa.

Descripción de Apartado Número Cuatro

Se aplica configuraciones que permitan detectar vínculos sospechosos a sitios web, así como manipulación indebida de en la información. Además, se activan notificaciones para recibir alertas de seguridad ante eventos que representen un riesgo para la información almacenada en la nube.

Manual para la Configuración de Alertas de Seguridad y Detección de Actividades Sospechosas en la Gestión Documental en la Nube

Objetivo

Establecer un procedimiento para configurar mecanismos de monitoreo y alertas de seguridad que permitan detectar accesos sospechosos, vínculos maliciosos, modificaciones no autorizadas en archivos y carpetas, así como cambios indebidos en permisos de acceso dentro de la plataforma de almacenamiento en la nube. Este manual busca fortalecer la protección de la información y facilitar una respuesta oportuna ante posibles incidentes de seguridad.

Alcance

Este manual aplica a:

a) Usuarios internos.

b) Usuarios externos autorizados.

c) Administradores de sistemas.

d) Documentos y carpetas almacenados en la nube.

e) Sistemas de gestión documental.

f) Herramientas de monitoreo y seguridad implementadas por la organización.

Responsables

Tabla 20

Responsables del monitoreo y la gestión de alertas de seguridad

Responsable	**Función**

Administrador de TI	Configurar alertas y monitoreo
Responsable de Seguridad de la Información	Supervisar eventos de seguridad
Jefaturas de Área	Reportar incidentes detectados
Usuarios Finales	Notificar actividades sospechosas

Nota. Elaboración propia, 2026

Configuración para la Detección de Vínculos Sospechosos

Descripción

Se configuran mecanismos de protección que permitan identificar enlaces potencialmente peligrosos compartidos en archivos, carpetas, correos electrónicos o plataformas colaborativas. Estas herramientas analizan la reputación de los sitios web y generan alertas cuando se detecten enlaces asociados con malware, phishing o actividades fraudulentas.

Procedimiento

a) Activar la protección contra phishing en la plataforma utilizada.

b) Habilitar el análisis automático de enlaces compartidos.

c) Configurar listas de sitios web bloqueados.

d) Restringir la apertura automática de enlaces externos.

e) Generar alertas cuando un usuario acceda a sitios considerados riesgosos.

f) Registrar todos los eventos relacionados con enlaces sospechosos.

Resultado Esperado

Identificar oportunamente intentos de fraude o robo de credenciales mediante enlaces maliciosos.

Configuración para la Detección de Manipulación de Información

Descripción

Se implementarán controles que permitan detectar modificaciones, eliminaciones o movimientos no autorizados de archivos y carpetas dentro del entorno documental. El objetivo es

garantizar la integridad de la información y prevenir pérdidas ocasionadas por errores o acciones maliciosas.

Procedimiento

a) Activar el historial de versiones de documentos.

b) Registrar cambios realizados sobre archivos y carpetas.

c) Habilitar auditorías de creación, edición y eliminación.

d) Configurar alertas por eliminación masiva de documentos.

e) Monitorear cambios en carpetas críticas.

f) Registrar la identidad del usuario que realizó la modificación.

Resultado Esperado

Detectar rápidamente actividades que comprometan la integridad de la documentación.

Configuración de Alertas por Cambios de Permisos

Descripción

Este control permitirá identificar modificaciones realizadas en los permisos de acceso de usuarios internos y externos, evitando que terceros alteren configuraciones de seguridad sin autorización.

Procedimiento

a) Activar el registro de cambios de permisos.

b) Configurar notificaciones automáticas para administradores.

c) Generar alertas cuando se otorguen privilegios administrativos.

d) Detectar cambios en permisos de carpetas críticas.

e) Registrar fecha, hora y usuario responsable.

f) Revisar periódicamente los eventos generados.

Resultado Esperado

Mantener control sobre la asignación y modificación de permisos de acceso.

Configuración de Notificaciones de Seguridad

Descripción

Las notificaciones de seguridad permiten informar de manera inmediata sobre eventos que representen una amenaza para la información o los sistemas de almacenamiento en la nube.

Procedimiento

a) Definir los eventos que generarán alertas.
b) Configurar el envío de notificaciones por correo electrónico.
c) Establecer destinatarios responsables de atender incidentes.
d) Configurar alertas para accesos fuera de horario laboral.
e) Activar avisos por intentos fallidos de autenticación.
f) Generar reportes automáticos de incidentes detectados.

Resultado Esperado

Permitir una respuesta rápida ante situaciones que representen riesgos para la seguridad de la información.

Eventos que Deben Generar Alertas

Tabla 21

Eventos que deben generar alertas de seguridad

Evento Detectado	**Nivel de Riesgo**	**Acción Recomendada**
Cambio de permisos administrativos	Alto	Revisar y validar autorización
Eliminación masiva de archivos	Alto	Iniciar investigación inmediata
Acceso desde ubicación inusual	Alto	Verificar identidad del usuario
Compartición externa no autorizada	Alto	Revocar acceso inmediatamente
Intentos fallidos repetitivos de acceso	Medio	Bloquear cuenta temporalmente
Descarga masiva de documentos	Alto	Analizar actividad del usuario

Modificación de carpetas críticas	Alto	Revisar cambios realizados
Acceso a enlaces sospechosos	Alto	Bloquear acceso y analizar evento

Nota. Elaboración propia, 2026

Revisión Periódica de Alertas

Descripción

El administrador de TI debe revisar periódicamente las alertas generadas por el sistema para verificar su validez y determinar las acciones correctivas necesarias. Esta revisión permite identificar patrones de comportamiento inusual, corregir vulnerabilidades y mejorar continuamente los controles de seguridad implementados. Los eventos críticos deben ser documentarse y escalarlos según el procedimiento de gestión de incidentes de la organización. Asimismo, se generan informes periódicos que permitan evaluar la efectividad de las alertas configuradas y realizar ajustes cuando sea necesario.

Frecuencia

a) Eventos críticos: revisión inmediata.
b) Eventos de riesgo medio: revisión semanal.
c) Revisión general de alertas: mensual.

Indicadores de Seguimiento

Tabla 22

Indicadores de seguimiento del monitoreo de alertas de seguridad

Indicador	**Fórmula**	**Meta**
Alertas atendidas	Alertas atendidas / Alertas generadas × 100	100%
Incidentes detectados oportunamente	Incidentes detectados / Incidentes reportados × 100	95%
Cambios de permisos monitoreados	Cambios monitoreados / Cambios realizados × 100	100%
Eventos sospechosos investigados	Eventos investigados / Eventos detectados × 100	100%

Nota. Elaboración propia, 2026

La implementación de este manual permite fortalecer la seguridad de la documentación en la nube mediante la detección temprana de accesos sospechosos, vínculos maliciosos y modificaciones indebidas de archivos o permisos. Asimismo, proporciona un mecanismo de

monitoreo continuo y generación de alertas que reducen el riesgo de alteración de permisos por usuarios externos, contribuyendo a la confidencialidad, integridad y disponibilidad de la información organizacional.

Gestión y Administración de Configuraciones Documentales Basada en ITIL

Problemas de gestión de configuraciones y datos distribuidos

Descripción del Problema

La administración de configuraciones y datos en el entorno del servidor puede ser complicada y propensa a errores, debido a que depende de un administrador remoto encargado de múltiples ubicaciones y sistemas.

Descripción del Apartado

Elaborar una política que establezca un marco de trabajo para la gestión y control de configuraciones y activos, con un enfoque flexible y práctico mediante los siguientes componentes:

a) Centralización de la gestión.
b) Automatización de procesos.
c) Auditoría y control.

Política de Gestión y Control de Configuraciones y Activos Tecnológicos para la Administración de Documentación en la Nube

Objetivo

Establecer un marco de trabajo para la gestión, control y monitoreo de las configuraciones y activos tecnológicos relacionados con la documentación en la nube, garantizando una administración centralizada, automatizada y auditable que reduzca errores operativos, fortalezca la seguridad de la información y facilite la administración de múltiples ubicaciones y sistemas.

Alcance

Esta política aplica a:

a) Servidores físicos y virtuales.
b) Plataformas de almacenamiento en la nube.
c) Sistemas de gestión documental.
d) Equipos de cómputo utilizados para la administración.
e) Aplicaciones relacionadas con la documentación.

f) Configuraciones de seguridad.
g) Usuarios internos y administradores externos autorizados.

Justificación

La gestión de configuraciones y datos distribuidos puede generar inconsistencias, errores de administración y dificultades para mantener el control de los recursos tecnológicos cuando existen múltiples ubicaciones o administradores responsables. Por ello, se requiere una política que permita centralizar la administración, automatizar tareas repetitivas y establecer mecanismos de auditoría que garanticen la integridad, disponibilidad y confiabilidad de la información.

Principios de la Política

Centralización de la Gestión

Toda configuración relacionada con los sistemas de documentación en la nube deberá administrarse desde una plataforma centralizada que permita controlar usuarios, permisos, dispositivos y servicios desde un único punto de gestión.

Automatización de Procesos

Las actividades repetitivas de administración deben automatizarse mediante herramientas tecnológicas que reduzcan errores humanos y mejoren la eficiencia operativa.

Auditoría y Control

Toda modificación realizada sobre configuraciones, activos y recursos tecnológicos deben registrarse y mantenerse disponible para procesos de auditoría, seguimiento e investigación.

Lineamientos de Centralización de la Gestión

Administración Centralizada

La organización debe implementar una consola o plataforma de administración centralizada que permita gestionar todos los recursos documentales y tecnológicos desde un único entorno. Esta medida facilitará la supervisión de múltiples ubicaciones, permitirá aplicar configuraciones uniformes y reducirá la dependencia de procesos manuales. Asimismo, toda modificación relevante deberá realizarse únicamente desde las herramientas autorizadas por la organización para garantizar el control y la trazabilidad de los cambios efectuados.

Inventario Centralizado de Activos

Se mantendrá un inventario actualizado de todos los activos tecnológicos asociados con la gestión documental. Dicho inventario debe incluir servidores, aplicaciones, dispositivos, usuarios administrativos, configuraciones críticas y recursos de almacenamiento en la nube. La actualización constante de esta información permitirá identificar activos obsoletos, detectar configuraciones no autorizadas y facilitar la gestión de incidentes relacionados con la infraestructura tecnológica.

Estandarización de Configuraciones

Todas las configuraciones deben definirse mediante plantillas y estándares previamente aprobados por el área de tecnología de la información. Esto permitirá asegurar que los sistemas mantengan niveles homogéneos de seguridad, funcionamiento y disponibilidad. Además, cualquier excepción deberá ser documentada, justificada y aprobada por el responsable de la gestión tecnológica.

Lineamientos de Automatización de Procesos

Automatización de Configuraciones

La organización proveer el uso de herramientas que permiten desplegar, actualizar y corregir configuraciones de forma automática. La automatización reducirá la probabilidad de errores humanos y garantizará que los cambios se apliquen de manera uniforme en todos los sistemas administrados. Asimismo, deberá existir una validación previa antes de ejecutar cambios masivos que puedan afectar la operación de los servicios.

Automatización de Copias de Seguridad

Los respaldos de configuraciones, bases de datos y documentación deben ejecutarse de forma automática según la frecuencia establecida por la organización. Estos respaldos deberán almacenarse en ubicaciones seguras y verificarse periódicamente para garantizar su correcta recuperación en caso de incidentes o fallos operativos.

Automatización de Alertas

Se implementarán mecanismos automáticos de notificación para informar sobre cambios no autorizados, errores de configuración, accesos sospechosos o eventos que representen riesgos

para la infraestructura tecnológica. Las alertas deben enviarse a los responsables definidos para asegurar una respuesta rápida y efectiva.

Lineamientos de Auditoría y Control

Registro de Cambios

Toda modificación realizada sobre configuraciones, permisos, aplicaciones o activos tecnológicos debe quedar registrada en una bitácora centralizada. El registro tiene que contener información sobre el usuario responsable, fecha, hora, descripción del cambio y justificación correspondiente. Esta información será utilizada para procesos de auditoría y seguimiento.

Auditorías Periódicas

Se realizan auditorías periódicas para verificar que las configuraciones implementadas correspondan a los estándares establecidos por la organización. Durante estas revisiones se evaluarán permisos, configuraciones de seguridad, activos tecnológicos y cumplimiento de procedimientos internos. Los hallazgos identificados tienen que documentarse y corregirse oportunamente.

Control de Versiones

Las configuraciones críticas deben mantenerse bajo un esquema de control de versiones que permita identificar cambios realizados a lo largo del tiempo. Este mecanismo facilitará la recuperación de configuraciones anteriores en caso de errores o incidentes que afecten la operación de los servicios.

Monitoreo Continuo

La organización deberá implementar herramientas de monitoreo que permitan supervisar el estado de las configuraciones y activos tecnológicos en tiempo real. Estas herramientas facilitan la detección temprana de incidentes y contribuirán a mantener la estabilidad de la infraestructura.

Roles y Responsabilidades

Tabla 23

Roles y responsabilidades para la gestión de configuraciones y activos tecnológicos

Responsable	**Función**
Administrador de TI.	Gestionar configuraciones y activos tecnológicos.
Responsable de Seguridad de la Información.	Supervisar el cumplimiento de la política
Jefaturas de Área.	Autorizar cambios relevantes.
Usuarios Autorizados.	Cumplir los procedimientos establecidos.
Auditor Interno.	Verificar la correcta aplicación de los controles.

Nota. Elaboración propia, 2026

Indicadores de Cumplimiento

Tabla 24

Indicadores de cumplimiento de la política de gestión de configuraciones y activos tecnológicos

Indicador	**Meta**
Configuraciones registradas en inventario	100 %
Cambios documentados	100 %
Copias de seguridad ejecutadas correctamente	100 %
Auditorías realizadas según cronograma	100 %
Incidentes por errores de configuración	Menor al 5 % anual
Activos actualizados en inventario	100 %

Nota. Elaboración propia, 2026

Resultados Esperados

a) Centralización de la administración de configuraciones y activos.

b) Reducción de errores operativos derivados de la gestión manual.
c) Mayor control sobre los recursos tecnológicos distribuidos.
d) Mejor capacidad de monitoreo y respuesta ante incidentes.
e) Incremento de la trazabilidad y la transparencia de los cambios realizados.
f) Fortalecimiento de la seguridad y continuidad de la gestión documental en la nube.
g) Optimización de la administración de múltiples ubicaciones y sistemas bajo una metodología uniforme y controlada.

Control de Versiones y Capacitación en la Gestión Documental en Microsoft OneDrive

Pérdida de información.

Descripción del Problema

Se genera la pérdida de información por varias razones, a menudo relacionadas con problemas de hardware, software, red o errores de usuarios.

Descripción de Apartado Número Uno

Configurar la plataforma de nube para que mantenga un historial de cada archivo.

Manual de Controles para la Gestión y Conservación del Historial de Versiones de Archivos en la Nube

Objetivo

Establecer los controles y procedimientos necesarios para configurar la plataforma de almacenamiento en la nube de manera que mantenga un historial de versiones de cada archivo, permitiendo recuperar información modificada, eliminada o dañada por errores de usuarios, fallos de software, problemas de hardware o incidentes de seguridad.

Alcance

Este manual aplica a:

a) Documentos almacenados en la nube.
b) Carpetas compartidas.
c) Usuarios internos.
d) Usuarios externos autorizados.

e) Administradores de la plataforma.
f) Sistemas de gestión documental.

Justificación

La pérdida de información representa uno de los riesgos más importantes para la gestión documental en la nube. Las modificaciones incorrectas, las eliminaciones accidentales, los ataques informáticos o los fallos tecnológicos pueden afectar la disponibilidad e integridad de los documentos. Por esta razón, es necesario implementar controles que permitan conservar el historial de cada archivo, facilitando la recuperación de versiones anteriores y garantizando la continuidad de las operaciones.

Controles de Configuración del Historial de Archivos

Control 1. Activación del Historial de Versiones

Objetivo

Garantizar que todos los archivos almacenados en la plataforma mantengan un registro de las modificaciones realizadas.

Procedimiento

a) Ingresar a la consola de administración de la plataforma.
b) Acceder a la configuración de gestión documental.
c) Habilitar la opción "Control de versiones" o "Historial de versiones".
d) Configurar la aplicación automática para todas las bibliotecas y carpetas.
e) Verificar que cada modificación genere una nueva versión del archivo.
f) Documentar la activación realizada.

Resultado Esperado. Cada archivo almacenará automáticamente un historial completo de cambios realizados por los usuarios.

Control 2. Conservación de Versiones Históricas

Objetivo

Mantener disponibles versiones anteriores para recuperación ante incidentes.

Procedimiento

a) Definir la cantidad mínima de versiones a conservar.

b) Configurar la retención automática de versiones.
c) Establecer períodos de conservación según la criticidad de la información.
d) Evitar la eliminación automática de versiones importantes.
e) Revisar periódicamente el cumplimiento de la retención configurada.

Resultado Esperado: Disponibilidad de versiones anteriores para restaurar información cuando sea necesario.

Control 3. Registro de Cambios por Usuario

Objetivo

Identificar quién realizó modificaciones sobre los documentos.

Procedimiento

a) Activar los registros de auditoría.
b) Asociar cada cambio a una cuenta de usuario.
c) Registrar fecha y hora de las modificaciones.
d) Almacenar el historial de actividades.
e) Restringir la alteración de los registros de auditoría.

Resultado Esperado: Trazabilidad completa de todas las acciones realizadas sobre los documentos.

Control 4. Recuperación de Versiones Anteriores

Objetivo

Permitir la restauración rápida de archivos modificados o eliminados incorrectamente.

Procedimiento

a) Habilitar la función de restauración de versiones.
b) Asignar permisos de recuperación a administradores autorizados.
c) Verificar que las versiones restauradas mantengan su integridad.
d) Documentar cada restauración realizada.
e) Validar periódicamente el funcionamiento del proceso.

Resultado Esperado. Recuperación eficiente de información ante errores o incidentes.

Control 5. Protección Contra Eliminación Definitiva

Objetivo

Evitar la pérdida permanente de documentos importantes.

Procedimiento

a) Activar la papelera de reciclaje de la plataforma.
b) Configurar períodos de retención para archivos eliminados.
c) Impedir la eliminación definitiva por usuarios estándar.
d) Mantener copias temporales antes de la eliminación permanente.
e) Realizar revisiones periódicas de los elementos eliminados.

Resultado Esperado: Reducción significativa del riesgo de pérdida permanente de información.

Control 6. Monitoreo de Cambios Masivos

Objetivo

Detectar actividades que puedan afectar grandes volúmenes de información.

Procedimiento

a) Configurar alertas para modificaciones masivas.
b) Generar notificaciones por eliminación de múltiples archivos.
c) Monitorear cambios realizados fuera del horario laboral.
d) Registrar actividades sospechosas.
e) Escalar incidentes al responsable de seguridad.

Resultado Esperado: Detección temprana de errores o actividades maliciosas.

Procedimiento de Revisión del Historial

Descripción

El administrador de la plataforma debe revisar periódicamente el historial de versiones para verificar que las configuraciones continúen funcionando correctamente. Durante la revisión, se comprobará que los documentos registren nuevas versiones cuando sean modificados, que los registros de auditoría se mantengan disponibles y que las funciones de recuperación operen adecuadamente. Asimismo, se identifican errores de configuración, fallos de sincronización o problemas que puedan afectar la conservación del historial documental. Los resultados de la

revisión deben documentarse y toda la anomalía detectada ser corregirse oportunamente para garantizar la protección de la información.

Frecuencia

a) Revisión operativa: Mensual.
b) Verificación de restauración: Trimestral.
c) Auditoría general: Semestral.

Roles y Responsabilidades

Tabla 25

Roles y responsabilidades para la revisión del historial de versiones

Responsable	Función	Responsable
Administrador de TI	Configurar y supervisar el historial de versiones	Administrador de TI
Responsable de Seguridad de la Información	Verificar el cumplimiento de los controles	Responsable de Seguridad de la Información
Jefaturas de Área	Autorizar restauraciones de documentos críticos	Jefaturas de Área
Usuarios Finales	Utilizar adecuadamente las herramientas documentales	Usuarios Finales
Auditor Interno	Revisar la efectividad de los controles implementados	Auditor Interno

Nota. Elaboración propia, 2026

Indicadores de Cumplimiento

Tabla 26

Indicadores de cumplimiento para la gestión del historial de versiones

Indicador	Fórmula	Meta
Archivos con historial activo	Archivos con historial / Total de archivos × 100	100 %
Versiones recuperadas exitosamente	Recuperaciones exitosas / Recuperaciones realizadas × 100	100 %
Incidentes de pérdida de información	Total, de incidentes reportados	Tendencia decreciente
Revisiones ejecutadas	Revisiones realizadas / Revisiones programadas × 100	100 %
Archivos protegidos por retención	Archivos protegidos / Total de archivos × 100	100 %

Nota. Elaboración propia, 2026

Descripción de Apartado Número Dos

Capacitar a los empleados en el uso seguro y adecuado de la plataforma en la nube, destacando la importancia de seguir los protocolos de acceso y edición.

Manual de Capacitación para el Uso Seguro, Acceso y Edición de Documentos en la Nube

Objetivo

Capacitar a los colaboradores de la organización en el uso seguro y adecuado de la plataforma de almacenamiento en la nube, promoviendo buenas prácticas para el acceso, edición, almacenamiento y protección de la información, con el fin de reducir el riesgo de pérdida de datos ocasionada por errores humanos, accesos inadecuados o incumplimiento de los procedimientos establecidos.

Alcance

Este manual aplica a:

- Personal administrativo.
- Personal operativo.
- Jefaturas y supervisores.
- Usuarios con acceso a la plataforma de nube.
- Colaboradores internos y externos autorizados.

Justificación

La pérdida de información puede producirse por errores en la manipulación de archivos, eliminación accidental de documentos, uso incorrecto de permisos o desconocimiento de las funcionalidades de la plataforma de nube. Por esta razón, resulta necesario establecer un programa de capacitación que permita a los usuarios conocer los procedimientos adecuados para acceder, editar y proteger la documentación institucional, fortaleciendo así la seguridad y disponibilidad de la información.

Normas Generales para el Uso de la Nube

Uso de Credenciales Personales

Cada colaborador debe utilizar únicamente las credenciales asignadas por la organización para acceder a la plataforma de nube. Las cuentas son personales e intransferibles; por lo tanto, queda prohibido compartir usuarios o contraseñas con otros colaboradores o terceros. Asimismo, las credenciales deben mantenerse protegidas mediante contraseñas seguras y mecanismos de autenticación adicionales cuando estén disponibles.

Protección de la Información

Los usuarios deben manipular la documentación institucional siguiendo los niveles de acceso asignados. Ningún colaborador podrá copiar, compartir, descargar o modificar información para la cual no posea autorización. La protección de la información es una responsabilidad compartida y forma parte de las obligaciones laborales de cada usuario.

Uso Exclusivo para Fines Laborales

La plataforma de nube deberá utilizarse únicamente para actividades relacionadas con las funciones de la organización. El almacenamiento de archivos personales o información ajena a las actividades institucionales deberá evitarse para reducir riesgos de seguridad y optimizar el uso de los recursos tecnológicos.

Procedimiento para el Acceso Seguro a la Nube

Descripción

Antes de acceder a la plataforma, los usuarios deberán verificar que se encuentran utilizando dispositivos autorizados y conexiones seguras. El acceso debe realizarse únicamente a través de los medios establecidos por la organización, evitando enlaces desconocidos o páginas web no oficiales. Asimismo, los colaboradores deben cerrar sesión cuando finalicen sus actividades, especialmente cuando utilicen equipos compartidos o ubicados fuera de las instalaciones de la empresa. Estas medidas ayudan a prevenir accesos no autorizados y protegen la información almacenada en la nube.

Recomendaciones

a) Utilizar contraseñas robustas.

b) Activar la autenticación multifactor cuando esté disponible.
c) No guardar contraseñas en equipos públicos.
d) Cerrar sesión al finalizar las actividades.
e) Reportar inmediatamente accesos sospechosos.

Procedimiento para la Edición Correcta de Documentos

Descripción

Antes de modificar un documento, el usuario debe verificar que se encuentra trabajando sobre la versión correcta del archivo y que cuenta con los permisos necesarios para realizar cambios. Toda edición debe efectuarse respetando la estructura documental establecida por la organización. Asimismo, se recomienda revisar cuidadosamente los cambios antes de guardar la información para evitar errores que puedan afectar la integridad de los documentos. Cuando existan funciones de control de versiones, los usuarios deberán utilizarlas para mantener un historial adecuado de las modificaciones realizadas.

Recomendaciones

a) Verificar la versión del documento antes de editar.
b) Evitar modificar documentos sin autorización.
c) Revisar los cambios antes de guardar.
d) Utilizar nombres de archivo estandarizados.
e) Mantener la estructura de carpetas definida por la organización.

Procedimiento para Evitar la Pérdida de Información

Descripción

Los colaboradores deben adoptar prácticas que minimicen el riesgo de pérdida de documentos y datos importantes. Entre estas prácticas se encuentra evitar la eliminación innecesaria de archivos, utilizar las funciones de recuperación disponibles y verificar periódicamente que los documentos se encuentren sincronizados correctamente con la nube. Además, cualquier incidente relacionado con pérdida de información deberá ser reportado de forma inmediata al área de tecnología para su análisis y recuperación.

Recomendaciones

a) No eliminar archivos sin validación previa.
b) Utilizar la papelera de reciclaje cuando sea necesario.
c) Verificar la sincronización de documentos.
d) Mantener actualizadas las aplicaciones utilizadas.
e) Reportar errores de almacenamiento inmediatamente.

Capacitación en Seguridad de la Información

Descripción

La organización desarrollará sesiones periódicas de capacitación para fortalecer los conocimientos de los colaboradores sobre el uso seguro de la nube. Estas actividades incluirán temas relacionados con protección de contraseñas, identificación de correos fraudulentos, manejo adecuado de documentos, control de accesos y prevención de incidentes de seguridad. La capacitación continua permitirá reducir errores humanos y fomentar una cultura organizacional orientada a la protección de la información.

Temas de Capacitación

a) Uso seguro de la nube.
b) Gestión de contraseñas.
c) Control de accesos y permisos.
d) Identificación de amenazas informáticas.
e) Recuperación de documentos.
f) Buenas prácticas de seguridad documental.

Responsabilidades de los Usuarios

Tabla 27
Responsabilidades de los usuarios en la gestión documental en la nube

Responsabilidad	**Descripción**
Proteger credenciales	Mantener seguras las cuentas de acceso
Cumplir procedimientos	Seguir las normas establecidas por la organización
Proteger documentos	Evitar modificaciones o eliminaciones indebidas
Reportar incidentes	Informar situaciones de riesgo o pérdida de información

Participar en capacitaciones	Asistir a los programas de formación establecidos

Nota. Elaboración propia, 2026

Evaluación del Conocimiento

Para verificar la efectividad de la capacitación, la organización evaluará periódicas al colaborador para medir el nivel de comprensión de los colaboradores respecto a las normas y procedimientos establecidos. Los resultados obtenidos servirán para identificar necesidades de capacitación adicionales y fortalecer los aspectos que presenten mayores dificultades entre los usuarios.

Frecuencia

a) Capacitación general: Semestral.
b) Refuerzo de seguridad: Trimestral.
c) Evaluación de conocimientos: Anual.

Indicadores de Cumplimiento

Tabla 28
Indicadores de cumplimiento de la capacitación en seguridad de la información

Indicador	**Meta**
Colaboradores capacitados	100 %
Participación en capacitaciones	95 % o superior
Incidentes por errores de usuario	Tendencia decreciente
Evaluaciones aprobadas	90 % o superior
Reportes oportunos de incidentes	100 %

Nota. Elaboración propia, 2026

CAPÍTULO VI: CONCLUSIONES

La investigación permitió identificar que el modelo actual de gestión documental de Golden Comunicaciones S.A., basado en un servidor NAS ubicado fuera del país, presenta limitaciones significativas relacionadas con bloqueos de archivos, pérdida de información, problemas de acceso remoto, conflictos de edición y dependencia de conexiones VPN, afectando directamente la productividad y eficiencia de los colaboradores.

El análisis teórico demostró que la adopción de plataformas de almacenamiento en la nube constituye una alternativa viable para mejorar la administración documental, ya que ofrecen mecanismos de control de versiones, respaldo automático, gestión de permisos, disponibilidad de la información y acceso seguro desde múltiples ubicaciones.

Asimismo, el estudio evidenció que la implementación de una metodología basada en Microsoft OneDrive, alineada con las buenas prácticas de ISO 27001, ISO 9001 e ITIL, fortalece los principios de confidencialidad, integridad y disponibilidad de la información, contribuyendo a una gestión documental más segura y controlada.

Los resultados obtenidos mediante la observación y las entrevistas permitieron confirmar la existencia de problemas operativos que afectan el trabajo colaborativo, principalmente debido a la ausencia de control de versiones automatizado, limitaciones en el acceso simultáneo a documentos y procesos manuales de recuperación de información.

Se determinó que la empresa dispone de la infraestructura tecnológica, las licencias corporativas y los recursos operativos necesarios para implementar la propuesta metodológica sin requerir inversiones significativas en hardware o software adicional, lo que garantiza la viabilidad técnica, operativa y económica del proyecto.

La propuesta metodológica diseñada permite atender los objetivos específicos planteados mediante la incorporación de controles de bloqueo, procedimientos de gestión de daños, controles de seguridad, autenticación de usuarios, revisión periódica de permisos, alertas de seguridad y mecanismos de recuperación de información.

La migración de la gestión documental hacia un entorno en la nube constituye una estrategia de transformación digital que no solo mejora la administración de la información, sino que también incrementa la competitividad organizacional al optimizar los tiempos de respuesta, facilitar las auditorías y fortalecer la continuidad operativa de la empresa.

Finalmente, se concluye que la metodología propuesta constituye una solución efectiva para reducir los riesgos asociados a la pérdida de información, mejorar la colaboración entre los usuarios y establecer una estructura documental más organizada, segura y alineada con los estándares internacionales de gestión de la información, generando beneficios sostenibles para Golden Comunicaciones S.A.

CAPÍTULO VII: RECOMENDACIONES

Con base en los resultados de la investigación, se recomienda a Golden Comunicaciones S.A. implementar de forma gradual la metodología de gestión documental basada en Microsoft OneDrive, ya que permitirá solucionar los problemas de bloqueo de archivos, pérdida de información y dificultades de acceso identificados en el sistema actual. Una implementación progresiva facilitará la adaptación de los colaboradores y reducirá riesgos durante el proceso de migración.

Asimismo, se recomienda fortalecer la capacitación del personal en el uso de Microsoft OneDrive y en las buenas prácticas de seguridad de la información, con el fin de disminuir errores humanos y garantizar un adecuado aprovechamiento de las herramientas de colaboración, control de versiones y gestión documental.

También se recomienda implementar de manera formal las políticas y procedimientos de control de versiones, permisos y seguridad propuestos en la investigación, ya que contribuirán a proteger la información, mejorar la trazabilidad de los documentos y facilitar el cumplimiento de las buenas prácticas establecidas por las normas ISO 27001, ISO 9001 e ITIL.

Finalmente, se concluye que la implementación de Microsoft OneDrive es funcional y viable para Golden Comunicaciones S.A., debido a que la empresa ya dispone de la infraestructura tecnológica, las licencias de Microsoft 365 y el personal necesario para su adopción. Además, la plataforma permitirá optimizar la gestión documental, fortalecer la seguridad de la información, facilitar el trabajo colaborativo y mejorar la productividad sin requerir una inversión significativa.

REFERENCIAS

Artavia López, L. I. (2025). *Guía para la gestión de vulnerabilidades en la seguridad de la información según ISO/IEC 27001 para la empresa Energym, Guanacaste, Costa Rica* [Tesis]. Suwa Repositorio. https://repositorio.usam.ac.cr/xmlui/handle/111506/2872

Editorial Etece. (2025). *Fuentes de information*. Conceptos. https://concepto.de/fuentes-de-informacion/

ESGinnova Group (2026). *Blog especializado en gestion de Calidad. 7.5.* informacion documentada. https://www.nueva-iso-9001-2015.com/7-5-informacion-documentada/

Glosario de HPE (2025). Aquitectura de nube. ¿Que es la arquitectura de nube? https://www.hpe.com/lamerica/es/what-is/cloud-architecture.html?utm_source

Hernández Sampieri, R., Méndez Valencia, S., Mendoza Torres, C. P., & Cuevas Romo, A. (2017). *Fundamentos de investigación*. McGraw-Hill Education.

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements. ISO.*

ISO 9001:2015 – *Gestión de calidad (Microsoft Azure Compliance demuestra el estándar)*

ISO/IEC 27001 – *Seguridad de la información*

Martínez Piva, J. M. (Coord.). (2008). *Generación y protección del conocimiento: Propiedad intelectual, innovación y desarrollo económico.* Comisión Económica para América Latina y el Caribe (CEPAL). https://repositorio.cepal.org/items/8ad90f7c-c77d-4b99-a075-7d6186fa75a9

Peter M. Mell y Thimothy Grance (2011). *La definicion del NIST de computacion en la nube*. NIST. https://www.nist.gov/publications/nist-definition-cloud-computing

Porter, M. (1985). *Competitive Advantage*. *Creating and sustaining superior performance*. Free Press.

Wikipedia. (2022). *Razon fundamental*. ISO/IEC 27001. https://en.wikipedia.org/wiki/ISO/IEC_27001

ANEXOS

Anexo 1 Guia de Entrevista

Entidad:	Golden Comunicaciones S.A.
Nombre del entrevistado:	Tatiana Robledo
Puesto del entrevistado:	Gerente de Operaciones
Nombre del estudiante:	María Camila Figueroa Mora
Fecha de la entrevista:	
Lugar o medio de la entrevista:	De manera presencial, en la ubicación de Santa Ana, Pozos, Oficina.

Preguntas:

a) Área en la que labora:

1. Administrativa
2. Técnica
3. Tecnologías de la Información
4. Otra

b) Tiempo laborando en la empresa:

1. Menos de 1 año
2. 1 a 3 años
3. 4 a 6 años

4. Más de 6 años

c) ¿Utiliza el sistema de almacenamiento documental de la empresa?
    1. Sí
    2. No
d) Desde su experiencia, ¿qué dificultades ha encontrado al trabajar con el sistema actual de almacenamiento documental?
e) Describa una situación en la que haya tenido problemas al editar o compartir un documento con otros colaboradores.
f) ¿Cómo afecta el sistema actual su organización y gestión diaria de documentos?
g) ¿Qué mejoras considera necesarias en el sistema de gestión documental de la empresa?
h) ¿Qué expectativas tendría frente a un sistema de almacenamiento en la nube?
i) ¿Considera que la empresa requiere capacitación en gestión documental digital? Explique su respuesta.
j) ¿Desea agregar algún comentario adicional sobre el manejo actual de los documentos en la empresa?

Anexo 2 Guia de Observacion

GUÍA DE OBSERVACIÓN

Entidad:	**Golden Comunicaciones S.A.**
Dirección física de la entidad:	De momentum de lindora 300m al oeste, Centro corporativo lindora Oficina 306, Pozos, Santa Ana
Fecha de la actividad de observación:	
Nombre del estudiante:	Maria Camila Figueroa Mora

Tabla de control de aspectos observados:

No	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
1	Forma en que los usuarios acceden a los archivos y carpetas del sistema.				
2	Control de permisos y roles asignados a los usuarios para acceder a la información,				
3	Existencia de bloqueos o conflictos cuando varios usuarios editan en un mismo archivo.				
4	Uso del control de versiones para registrar cambios en los documentos.				

No	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
5	Procedimientos de respaldo o recuperación de archivos ante perdida de información.				
6	Organización y estructura de las carpetas dentro del sistema al almacenamiento.				
7	Existencia de alertas o notificaciones ante cambios o accesos sospechosos.				
8	Tiempo de acceso a los archivos y rendimiento del sistema al abrir documentos.				