



**UNIVERSIDAD
NACIONAL DE LOJA**

**FACULTAD DE LA EDUCACIÓN, EL ARTE Y COMUNICACIÓN
CARRERA DE PEDAGOGÍA DE LAS CIENCIAS
EXPERIMENTALES MENCIÓN INFORMÁTICA**

GESTIÓN DE TECNOLOGÍA EDUCATIVA

Tema:

FUNDAMENTACIÓN TEÓRICA

Protección, gestión y compartición de contenido digital.

Estudiantes:

Grace Stefania Soto Cango

Kevin Alejandro Morocho Morocho

Ciclo/Paralelo:

Ciclo VI

Periodo Académico:

LOJA – ECUADOR

2022 – 2023

Introducción

Fundamentación Teórica

En la era digital, la protección, gestión y compartición de contenido digital se han convertido en pilares fundamentales para el desarrollo y sostenibilidad de diversos sectores, incluyendo el educativo, empresarial y cultural. El rápido avance de las tecnologías de la información y comunicación ha facilitado el acceso y distribución de información a niveles sin precedentes, pero también ha planteado nuevos desafíos relacionados con la seguridad, integridad y privacidad de los datos.

Este informe tiene como objetivo proporcionar una fundamentación teórica sobre la protección, gestión y compartición de contenido digital. A lo largo del documento, se abordarán conceptos clave, marcos legales y éticos, así como tecnologías y prácticas recomendadas en este campo, la protección del contenido digital implica la implementación de medidas para salvaguardar la información contra accesos no autorizados, modificaciones maliciosas y pérdida de datos, la gestión del contenido digital se refiere a las estrategias y herramientas utilizadas para organizar, almacenar, recuperar y mantener información de manera eficiente y efectiva, la compartición del contenido digital, por su parte, se enfoca en las metodologías y plataformas que facilitan el intercambio seguro y controlado de información entre usuarios y sistemas.

El contexto actual exige una comprensión profunda de estos conceptos para enfrentar de manera adecuada las amenazas cibernéticas y garantizar la confiabilidad y disponibilidad del contenido digital. En resumen, este informe ofrecerá una visión integral de las bases teóricas que sustentan la protección, gestión y compartición de contenido digital, proporcionando una guía para la implementación de mejores prácticas en diversos contextos y aplicaciones.

¿Qué es una competencia digital docente?

La competencia digital docente se refiere al conjunto de habilidades, conocimientos y actitudes que un profesor necesita para integrar eficazmente las tecnologías digitales en su práctica educativa. Este concepto abarca diversas dimensiones, que incluyen el uso de herramientas digitales para la enseñanza y el aprendizaje, la gestión de entornos virtuales, la promoción de la alfabetización digital entre los estudiantes y el fomento de un uso seguro y ético de la tecnología. (ProFuturo, 2023)

Protección, gestión y compartición de contenido digital.

Estos temas son aspectos fundamentales dentro de la realización de recursos digitales:

- **La protección**, es la seguridad de contenidos digitales, es el uso de tecnologías y estrategias para controlar el acceso, copia y distribución de medios digitales, con el fin de prevenir la piratería y asegurar que los creadores reciban una compensación justa por su trabajo. (Torres, 2022)
- **Gestión**: Es una forma moderna de organizar la documentación empresarial y es una manera segura y sostenible de mantener los archivos. Realizar una gestión documental digital es una forma de organizar mejor los archivos corporativos, modernizando la documentación. (Sydle, 2023)
- **Compartición**: Para poder estudiar y entender las normas al compartir contenido digital se debe tomar en cuenta medidas muy puntuales, como propone Rubio (2020): La finalidad es que, al acabar el módulo, sea capaz de compartir “de forma activa información, contenidos y recursos a través de comunidades en línea, redes y plataformas de colaboración”. Aquí se fomenta que el profesor sea proactivo en difundir los recursos y los contenidos educativos.

Herramientas o métodos para encontrar contenidos digitales.

Las herramientas para esta búsqueda pueden ser repositorios educativos y las bases de datos científicos estas herramientas juegan un papel crucial en la preservación y difusión del conocimiento. Herramientas como:

- **Dialnet**: Es un portal de difusión de la producción científica hispana, especializado en ciencias humanas y sociales. Permite buscar documentos, recibir alertas y acceder a catálogos completos de revistas académicas .

- **Scielo:** Esta plataforma facilita el acceso abierto a artículos científicos, permitiendo la preservación y recuperación de la información. Es ampliamente utilizada para encontrar y gestionar contenidos educativos digitales.
- **Google académico:** Ofrece una búsqueda amplia de literatura académica, incluyendo artículos, tesis, libros y resúmenes de diversas disciplinas. Es una herramienta útil para encontrar fuentes confiables y relevantes en el ámbito

Protección de documentos, los riesgos comunes.

Malware: Malware es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras. (Torres, 2022)

Acceso no autorizado: Es cualquier punto de acceso inalámbrico que se ha instalado en la infraestructura cableada de una red sin el consentimiento del administrador o propietario de la red, proporcionando así acceso inalámbrico no autorizado a la infraestructura cableada de la red. (Rouse, 2024)

Robo de datos: El robo de datos o robo de información, es la transferencia o el almacenamiento ilegal de información personal, confidencial o financiera. Esto podría incluir contraseñas, códigos de software. El robo de datos se considera una vulneración grave de la seguridad y la privacidad de las personas y las organizaciones. (Kaspersky, 2024)

Importancia de utilizar contraseñas seguras y el cifrado de documentos.

Una contraseña segura es la principal barrera que impide que te hackeen la mayoría de tus cuentas en línea. Exponerte al robo de identidad y a la extorsión es un riesgo que nunca debes correr. Tendrás que crear contraseñas que puedan combatir los métodos modernos de robo de contraseñas. (Kaspersky, 2023)

La tecnología de cifrado ayuda a proteger los datos en todos los dispositivos, incluso durante la transferencia. Las medidas adicionales de seguridad como la autenticación avanzada ayudan a disuadir a los usuarios no autorizados, el cifrado ayuda.

Programas de seguridad actualizados.

Un software de seguridad informática es un programa que sirve para proteger la privacidad de la información contenida en un sistema informático. (Soler, 2023)

Ejemplos:

- **BITDEFENDER**
- **AVG**
- **MALWAREBYTES**

Los sistemas operativos, navegadores web, programas y aplicaciones son susceptibles de tener fallos de seguridad. Por este motivo, pueden necesitar ser actualizados, independientemente del dispositivo en el que se encuentren instalados. (Incibe, s.f)

REALIZAR COPIAS DE SEGURIDAD

Hacer copias de seguridad (backup) de tu sitio web es esencial, no sólo para protegerlo contra la pérdida o corrupción de datos, sino también para garantizar que tu web pueda seguir disponible en caso de desastres informáticos. (Kitdigital, s.f)

¿Por qué es importante la gestión de documentos digitales?

La gestión de documentos digitales es importante porque mejora la accesibilidad, organización, seguridad y eficiencia en el manejo de la información empresarial.

Principales riesgos del archivado tradicional de documentos.

La gestión y archivo digital de documentos, según (Sydle ,2023) también ayuda a eliminar algunos de los riesgos que conlleva el almacenamiento tradicional de documentos, con pilas y pilas de papel.

Ambientales

Los rayos solares son uno de los principales riesgos ambientales, ya que destruyen el papel y la tinta. Si un documento está expuesto al sol durante mucho tiempo, puede perder su autenticidad, ya que su contenido comienza a desvanecerse.

Físicos

Los riesgos físicos incluyen las temperaturas altas o bajas, la iluminación excesiva y la humedad. Para evitar problemas graves, el entorno debe estar climatizado, con una temperatura siempre entre 20°C y 22°C.

Químicos

El polvo excesivo o la contaminación del aire también pueden dañar los documentos – y estos factores no siempre se tienen en cuenta.

Biológicos

Hongos, roedores e insectos, como polillas y hormigas, pueden convertirse en un gran problema para los documentos. Los pequeños "agujeros" que aparecen al principio pronto se apoderan del papel, destruyendo por completo los archivos.

Humanos

Y, por supuesto, existe el riesgo del error humano. La gente puede manipular los documentos con poco o ningún cuidado, derramar agua y comida, guardarlos mal o simplemente no archivarlos.

Riesgos de seguridad

También es importante hablar de la inseguridad del archivado tradicional. Cualquiera puede acceder a los documentos, con el consiguiente riesgo de pérdida de documentos y fuga de datos.

Metadatos.

Los metadatos son información que se agrega a un documento o archivo digital para describir su contenido, estructura y contexto, por eso *Villar 2023* nos dice que son una especie de “etiqueta” que nos proporciona detalles cruciales para comprender, clasificar y recuperar información de manera eficiente.

Tipos de metadatos de documentos

- ❖ **Metadatos descriptivos:** se centran en proporcionar información sobre el contenido del documento.
- ❖ **Metadatos administrativos:** contienen información relacionada con la administración y gestión del documento.
- ❖ **Metadatos estructurales:** describen la organización y la relación entre las partes de un documento.
- ❖ **Metadatos técnicos:** son las características técnicas del documento digital, como tamaño de archivo, formato, resolución de imagen y metadatos de la cámara si la imagen es escaneada.

Herramientas para optimizar la gestión de documentos digitales.

- La firma electrónica es una auténtica revolución en la firma de documentos.
- Sistemas de gestión digital:

Existen sistemas diseñados para gestionar documentos digitales, que almacenan, actualizan y comparten archivos, según los niveles de acceso y privacidad establecidos por la empresa.

- Nube:

Esta tecnología es muy importante para la gestión de documentos digitales, ya que facilita el acceso, reduce la necesidad de hardware robusto y garantiza la seguridad de los archivos.

Sistema de gestión de documentos (DMS)

Un sistema o software de gestión documental DMS permite almacenar, archivar, organizar y buscar rápidamente grandes cantidades de documentos, además, este tipo de software es capaz de registrar, en tiempo real, las modificaciones realizadas por diversos usuarios en un entorno colaborativo, manteniendo un registro de las diversas versiones creadas y modificadas por diferentes usuarios (seguimiento del historial) mediante su ciclo de vida. (GAD Software, 2024)

Compartición de documentos digitales.

Para poder estudiar y entender las normas al compartir contenido digital se debe tomar en cuenta medidas muy puntuales, como propone Rubio (2020):

La finalidad es que, al acabar el módulo, sea capaz de compartir “de forma activa información, contenidos y recursos a través de comunidades en línea, redes y plataformas de colaboración”. Aquí se fomenta que el profesor sea proactivo en difundir los recursos y los contenidos educativos. También de ser un “evangelizador”, es decir, incentivar el uso de las herramientas disponibles entre los alumnos y el resto del equipo docente.

Para poder determinar cuáles son los beneficios de compartir documentos con contenido digital, Ace (2024) define:

¿Qué implica compartir documentos?

El intercambio de archivos es el proceso de transmisión o distribución de archivos digitales de un usuario o dispositivo a otro, estas soluciones permiten tanto a particulares como a organizaciones compartir, colaborar y acceder fácilmente a la información en varios dispositivos y desde distintos lugares.

¿Por qué es útil?

- El propósito de compartir archivos es permitir la colaboración, el intercambio de información y el fácil acceso a archivos entre diferentes dispositivos, ubicaciones y personas.

- Fomenta la colaboración al permitir que varios usuarios vean y trabajen en el mismo archivo, lo que mejora la productividad y la eficiencia.
- Ayuda a realizar copias de seguridad y a recuperar datos, garantizando la seguridad de los archivos importantes en caso de fallo del hardware o de acontecimientos inesperados.

Métodos de compartición:

Correo electrónico: Ventajas

Sabemos que tener una cuenta de correo electrónico es esencial para la comunicación, por ello GoDaddy (2021) detalla algunos beneficios y limitaciones:

Los beneficios del correo electrónico son muchos y constituyen una excelente razón para utilizar este método de comunicación.

- Comunicación rápida y eficiente.
- Facilidad de uso y almacenamiento.
- Accesibilidad global.
- Ecológico.
- Bajo costo.

Correo electrónico: Limitaciones

Usar el correo electrónico también puede conllevar algunos inconvenientes que es importante conocer:

- Sobrecarga de información.
- Falta de inmediatez.
- Posibles malentendidos
- Spam y correo no deseado

Plataformas de colaboración

Microsoft Teams: “Es una plataforma para la comunicación y colaboración entre personas de un mismo equipo, empresa u organización. Es una aplicación de mensajería que permite realizar reuniones virtuales, chatear, compartir archivos, y mucho más” (Nfon, 2022, párr.2).

Slack: Es una aplicación de mensajería corporativa para empresas que conecta a los diferentes equipos de una organización de una manera más flexible e inclusiva. Está diseñada para hacer más sencillo el trabajo entre las personas facilitando el envío de mensajes dentro y

fuera de la organización. (Clarcat, 2023, párr.3-4)

Referencias bibliográficas:

Torres, C. (07 de abril de 2022). *¿En qué consiste la seguridad digital? Definición y ejemplos*. Webdoxclm.com.

McAfee. (2020, May 15). *¿Qué es malware?* McAfee; McAfee. <https://www.mcafee.com/es-mx/antivirus/malware.html>

¿Qué es el cifrado de datos? Definición y explicación. (2024). Kaspersky. <https://latam.kaspersky.com/resource-center/definitions/encryption>

Consejos para generar contraseñas seguras y únicas. (13 de diciembre de 2023). Kaspersky. <https://latam.kaspersky.com/resource-center/threats/how-to-create-a-strong-password>

Soler, L. (20 de abril de 2023). *Los 3 mejores software de Seguridad Informática de 2024 para proteger los datos de tu empresa*. SoftDoit. <https://www.softwaredoit.es/software-seguridad/index.html>

Políticas de Seguridad. (10 de agosto de 2022). Evaluandosoftware.com. <https://www.evaluandosoftware.com/ciberseguridad/politicas-de-seguridad/>

Cascarano, M. (17 de marzo de 2022). *¿Cómo instalar Bitdefender Antivirus? Guía de instalación*. Licendi. <https://licendi.com/es/blog/como-instalar-bitdefender-antivirus-guia-de-instalacion/>

El mejor Anti-malware gratis 2023. (25 de septiembre de 2023). Reparar Ordenadores. <https://repararordenadores.com/el-mejor-anti-malware-gratis-2023/>

La importancia de las actualizaciones de seguridad. (s.f). Incibe. <https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/actualizaciones-de-seguridad#:~:text=Los%20sistemas%20operativos%2C%20navegadores%20web,el%20que%20>

[20se%20encuentren%20instalados.](#)