TECNOLÓGICO NACIONAL DE MÉXICO.

INSTITUTO TECNOLÓGICO DE TLAXIACO.

“Seguridad informática: Derechos, obligaciones y sanciones legales.”

Presenta:

Alumnos: Kevin Sánchez Hernández 18620310.

Javier Noé Cruz España 18620152.

Yael De Jesús Santiago Ortiz 21620147.

Proyecto: Revista Informativa.

Docente: Edward Osorio Salinas.

Carrera: Ingeniería en Sistemas computacionales.

TLAXIACO, OAXACA, DICIEMBRE DEL 2024.

INDICE*

Tabla de contenido

INTRODUCCIÓN

Nuestro objetivo es proporcionarte una visión clara y concisa de los desafíos y oportunidades que presenta la ciberseguridad. Ya seas un usuario casual de internet o un profesional de la tecnología, esta revista te ofrecerá información relevante y actualizada para que puedas tomar decisiones informadas y proteger tus datos.

En un mundo cada vez más digitalizado, la seguridad de nuestra información se ha convertido en una preocupación primordial. Desde los ataques de hackers hasta el robo de identidad, los riesgos cibernéticos acechan en cada rincón del internet. Nuestra revista se adentra en este complejo universo para ofrecerte las herramientas y conocimientos necesarios para proteger tus datos y navegar de manera segura por el ciberespacio.

Únete a nosotros en este viaje por el apasionante mundo de la ciberseguridad y descubre cómo salvaguardar lo que más valoras en la era digital.

CAPITULO 1 GENERALIDADES DEL PROYECTO

1.1. Problemas a resolver, priorizándolos

Nuestro objetivo es proporcionarte una visión clara y concisa de los desafíos y oportunidades que presenta la ciberseguridad. Ya seas un usuario casual de internet o un profesional de la

tecnología, esta revista te ofrecerá información relevante y actualizada para que puedas tomar decisiones informadas y proteger tus datos.

Analizar la importancia de la integridad de archivos y la auditoría en el marco de la seguridad informática, considerando los aspectos legales y técnicos involucrados.

1.2. Objetivos (general y específicos)

- Revisar la legislación mexicana en materia de ciberseguridad.
- Identificar las principales amenazas a la integridad de los archivos.
- Evaluar las medidas de seguridad implementadas en una organización (caso de estudio).
- Proponer recomendaciones para mejorar la seguridad informática en México.

1.3. Justificación:

La presente investigación busca contribuir al conocimiento sobre la seguridad informática, con un enfoque particular en la integridad de archivos y la auditoría. Al analizar el marco legal vigente y los desafíos actuales en materia de ciberseguridad, se pretende identificar las brechas existentes y proponer soluciones prácticas para mejorar la protección de los datos. Asimismo, se busca concientizar a la sociedad sobre la importancia de adoptar medidas de seguridad adecuadas para prevenir incidentes cibernéticos.

CAPÍTULO 2: MARCO TEÓRICO

MARCO TEÓRICO

Derechos: Los derechos de los usuarios de tecnologías de la información y la comunicación (TIC) en México están establecidos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[1]. Estos derechos incluyen la protección de la privacidad, la seguridad y la integridad de los datos personales.

Obligaciones: Las obligaciones de los responsables del tratamiento de datos personales en México están establecidas en la LFPDPPP[1]. Estas obligaciones incluyen la implementación de medidas de seguridad adecuadas para proteger los datos personales, la notificación de incidentes de seguridad y la realización de auditorías y evaluaciones de riesgo.

Sanciones legales: Las sanciones legales por incumplimiento de la LFPDPPP en México pueden incluir multas, suspensiones o revocaciones de licencias, y even-tualmente, sanciones penales [2]. Es importante destacar que la LFPDPPP establece un régimen de responsabilidad objetiva, lo que significa que los responsables del tratamiento de datos personales pueden ser sancionados por incumplimientos, independientemente de si hubo intención o no.

La seguridad informática es un componente clave en el contexto de la sociedad digital, especialmente en un país como México, donde el uso de tecnologías de información y comunicación (TIC) ha crecido exponencialmente. Este marco teórico se centra en tres pilares

fundamentales: los derechos de los usuarios, las obligaciones de los individuos y las instituciones, y las sanciones legales aplicables en caso de incumplimiento de la normativa.

1. Conceptos Básicos de Seguridad Informática

La seguridad informática se define como el conjunto de medidas técnicas, operativas y legales diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información almacenada o transmitida mediante sistemas digitales. Los principales objetivos son prevenir accesos no autorizados, mitigar riesgos de pérdida de datos y garantizar la protección de los derechos de los usuarios.

2. Derechos de los Usuarios

Los derechos de los usuarios en el ámbito de la seguridad informática en México están respaldados por diversas normativas, entre las que destacan:

Derecho a la privacidad: Protegido por el Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Los usuarios tienen derecho a que sus datos sean tratados con confidencialidad y utilizados únicamente para los fines autorizados.

Derecho a la información clara y veraz: Establecido en la Ley Federal de Protección al Consumidor (LFPC), este derecho garantiza que los usuarios puedan entender cómo se está utilizando su información.

Derecho a la seguridad digital: Implícito en diversas regulaciones y normas, este derecho busca proteger a los usuarios contra ciberataques, fraudes y vulneraciones.

3. Obligaciones de los Actores Involucrados

En México, las obligaciones en materia de seguridad informática recaen tanto en instituciones públicas como privadas, así como en los usuarios finales.

a) Obligaciones de las Instituciones

Cumplir con la legislación vigente: Organizaciones públicas y privadas deben implementar medidas de seguridad informática acordes con la LFPDPPP y otras normativas aplicables.

Adoptar medidas de protección: Esto incluye el uso de tecnologías seguras, encriptación, y protocolos que garanticen la confidencialidad y disponibilidad de la información.

Notificar incidentes de seguridad: La Ley de Seguridad Nacional y la Ley General de Transparencia y Acceso a la Información Pública establecen que las instituciones deben reportar ciberataques o violaciones de datos.

b) Obligaciones de los Usuarios

Usar de manera responsable los sistemas digitales: Esto incluye evitar la propagación de malware y cumplir con los términos de uso de plataformas digitales.

Proteger sus credenciales: Los usuarios deben garantizar la seguridad de contraseñas y dispositivos utilizados para acceder a servicios digitales.

Reportar actividades sospechosas: La denuncia de cibercrímenes es fundamental para mitigar riesgos y activar mecanismos legales.

4. Sanciones Legales en México

El marco legal mexicano contempla sanciones administrativas, civiles y penales para quienes incumplen las normativas de seguridad informática. Entre las leyes destacadas se incluyen:

Código Penal Federal:

El Artículo 211 bis sanciona el acceso no autorizado a sistemas y bases de datos con penas de 3 meses a 6 años de prisión y multas económicas.

El Artículo 168 establece sanciones para quienes desarrollen o distribuyan software malicioso.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares:

Establece multas de hasta 320,000 unidades de medida y actualización (UMAs) por el tratamiento indebido de datos personales.

Ley de Instituciones de Crédito:

Regula las responsabilidades de las entidades financieras en la protección de información sensible y prevención de fraudes digitales.

CAPITULO 3: DESARRROLLO

Procedimiento y actividades desarrolladas

1. Planeación

- Identificación del público objetivo

Estudiantes, profesionales de TI, empresarios y usuarios generales interesados en la ciberseguridad.

2. Investigación

Recopilación de información de la los temas:

- Derechos relacionados con la seguridad informática.
- Obligaciones de usuarios, empresas y autoridades.
- Sanciones legales por delitos informáticos.

Y para ello revisamos

- Leyes y normativas vigentes
- Revisar artículos académicos, informes oficiales y casos reales.

- Entrevistas y opiniones de expertos

3. Redacción

Organización de contenidos

Dividir la revista en secciones

Escritura de artículos

Revisión y edición

Corregir errores gramaticales, de estilo y verificar que la información sea precisa.

4. Diseño

Creación de un esquema visual

Definir el diseño de la portada, las secciones internas y el índice. Elegir una combinación de colores y fuentes atractivas, pero profesionales. Incluir diagramas, ilustraciones, imágenes relacionadas con seguridad informática y citas destacadas.

5. Revisión final

Validación del contenido

Revisar que toda la información esté actualizada y correcta.

6. Publicación

Publicar en formato digital

Compartir a través de redes sociales, sitios web y correos electrónicos.

CAPITULO 4: RESULTADOS

4.1. RESULTADOS

En esta sección se presentan los resultados obtenidos a lo largo del desarrollo del proyecto "Seguridad informática: Derechos, obligaciones y sanciones legales". Dichos resultados son el producto del análisis, diseño, investigación y desarrollo que conformaron cada una de las etapas del proyecto.

Estos resultados representan el cumplimiento de los objetivos planteados y su relación directa con las necesidades identificadas en el contexto de la ciberseguridad. Los elementos entregados buscan ser una contribución clara y valiosa tanto para la comunidad académica como para usuarios y profesionales de la tecnología.

*** Resultados Documentales:**
Incluye la documentación principal que respalda el proyecto, como análisis legislativos, resultados investigativos y descripciones de amenazas a la seguridad informática en México. Estos materiales reflejan la profundidad del estudio realizado para sustentar la revista.

Prototipo de la Revista Informativa:

- **Diseño del borrador de la portada en formato digital**: Prototipo de la revista estructurado con un diseño visual profesional y atractivo, optimizado para distribución digital

- **Contenido organizado en secciones:**
  - **Derechos de los usuarios en seguridad informática:** Explicación clara y comprensible de las garantías legales que tienen los usuarios respecto a sus datos personales.
  - **Obligaciones de las instituciones y los individuos:** Detalla los deberes específicos establecidos en la legislación, enfocándose en el rol de empresas, instituciones públicas y usuarios.
  - **Sanciones legales contempladas en la legislación mexicana:** Expone las penalizaciones asociadas al incumplimiento de las normativas, incluyendo multas y responsabilidades penales.

Normatividades y Regulaciones:

- **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP):** Análisis de esta legislación con enfoque en su aplicación y alcance en la protección de datos personales.
- **Sanciones legales por incumplimiento:** Revisión de los artículos clave relacionados con ciberseguridad y penalizaciones por actos ilícitos.

Guías de Orientación:

- **Para usuarios generales:** Pasos prácticos para proteger datos personales, como la configuración de contraseñas seguras, uso de antivirus y precauciones al navegar en línea.
- **Para organizaciones:** Pautas para cumplir con la legislación, como implementar auditorías de seguridad, proteger datos sensibles y reportar incidentes cibernéticos.

CAPITULO 5: CONCLUSIONES DE PROYECTO.

5.1. Conclusión del Proyecto

La revista informativa "Seguridad informática: Derechos, obligaciones y sanciones legales" representa una aportación significativa al campo de la ciberseguridad en México. Este proyecto no solo logró sintetizar información clave sobre normatividades vigentes, derechos de los usuarios y responsabilidades de las instituciones, sino que también identificó áreas críticas de mejora en la protección de datos personales.

Se cumplió el objetivo principal: proporcionar una herramienta educativa y accesible que aborde los desafíos cibernéticos contemporáneos. Además, los resultados obtenidos en términos de diseño, contenido y distribución digital reflejan un enfoque integral y profesional que conecta el análisis legal con aplicaciones prácticas, sensibilizando tanto a expertos como a la sociedad en general.

La hipótesis inicial, que planteaba una necesidad urgente de mejorar el conocimiento y las prácticas en ciberseguridad, se comprobó. Este proyecto permitió también identificar limitaciones actuales en la

implementación de regulaciones y sanciones legales en México, destacando la importancia de continuar investigando sobre el tema y fortaleciendo las políticas públicas.

5.1.2. Recomendaciones y Experiencia Profesional Adquirida

Como propuesta para futuras actividades, se puede mejorar la portada incluyendo el uso de las VPNS y la manera en que protegen los datos personales y la ubicación de los usuarios al igual que algo más de diseño si se le da seguimiento. También se recomienda ampliar el alcance del proyecto, incorporando análisis de casos prácticos y herramientas interactivas que mejoren la experiencia del lector. También sería valioso implementar talleres educativos basados en el contenido de la revista para sensibilizar a la población sobre ciberseguridad.

Agregar en la posteridad: **Aspectos Visuales y Multimedia:**
Incluir tablas comparativas, infografías y diagramas para explicar conceptos complejos de manera sencilla. Se destacan ilustraciones con ejemplos de mejores prácticas en ciberseguridad, y fotos relevantes para un diseño dinámico y visualmente atractivo.

En términos profesionales, esta experiencia contribuyó al desarrollo de competencias como la investigación documental, redacción técnica y diseño editorial, así como la capacidad de trabajar en equipo y gestionar un proyecto multidisciplinario. La elaboración de la revista no solo fortaleció habilidades teóricas, sino que también ofreció una perspectiva aplicada sobre cómo influir positivamente en la protección de datos en México.

5.1.3. Fuentes de información.

1. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2019). *Guía para la protección de datos personales*. Recuperado de https://inai.org.mx
2. Congreso de la Unión de México. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. México: Diario Oficial de la Federación. Recuperado de https://www.dof.gob.mx
3. Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4ª ed.). Pearson.
4. Shinder, D. L., & Shinder, M. J. (2020). *Professional's Guide to Cybersecurity in the Digital Age*. Sybex/Wiley.
5. Organización de los Estados Americanos (OEA). (2018). *Guía de seguridad cibernética para pequeñas y medianas empresas*. Recuperado de https://www.oas.org
6. Flores Muñoz, F., & Velázquez Moreno, A. (2019). "Impacto de la Ley de Protección de Datos en México: Desafíos y oportunidades". Revista Mexicana de Ciberseguridad, 5(3), 45-57.
7. International Organization for Standardization. (2013). *ISO/IEC 27001:2013 – Information security management systems*. ISO.
8. Martínez, R. F. (2021). *Ciberseguridad y derecho en México*. Tirant Lo Blanch.