Maestro Jersain Zadamig Llamas Covarrubias

Sumario

1. **Introducción**
2. **La función del notario en la era digital**
3. **Ciberseguridad y protección de datos en las notarías**
4. **Implementación de tecnologías digitales en el ámbito notarial**
5. **Riesgos emergentes en la ciberseguridad para notarías**
6. **Mejores prácticas en ciberseguridad para notarías**
7. **Referencias**

Introducción

El notario ha sido históricamente una figura central en la protección de la seguridad jurídica, garantizando la autenticidad, legalidad y validez de documentos mediante la certificación presencial. Sin embargo, con la irrupción de la tecnología y la digitalización de procesos, el rol del notario ha comenzado a transformarse. La digitalización ha introducido nuevas dinámicas en la autenticación y gestión de documentos, requiriendo la adaptación de los notarios a un entorno donde la ciberseguridad y la protección de datos personales son esenciales para mantener la confianza en sus servicios.

En este contexto, surge el concepto de *Cyber Notary,* que se refiere a la integración de tecnologías digitales, como la firma electrónica y el *blockchain,* en las funciones notariales tradicionales. Estas herramientas permiten validar la autenticidad de documentos en entornos digitales, pero también plantean desafíos importantes, como la prevención del fraude, la manipulación de datos y el cumplimiento de normativas de protección de datos.

Este capítulo introductorio aborda la transformación del notariado en la era digital, explorando cómo la ciberseguridad se ha vuelto un pilar fundamental en la práctica notarial. Se analizarán los principales desafíos y oportunidades que presenta la digitalización para los notarios, con un enfoque en la implementación de medidas tecnológicas que garanticen la protección de la información confidencial y la seguridad de las transacciones electrónicas. Además, se expondrá el marco normativo que regula estas actividades, con especial atención a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento, los cuales imponen estrictas obligaciones a los notarios para asegurar el manejo adecuado de la información personal en el entorno digital.

En definitiva, el objetivo de este capítulo es proporcionar un panorama general de cómo la digitalización está redefiniendo el papel del notario, subrayando la importancia de la ciberseguridad en la protección de los documentos y datos sensibles que gestionan, y destacando la necesidad de una adaptación continua a las nuevas tecnologías para asegurar la seguridad jurídica en la era digital.

La función del notario en la era digital

El notario ha sido, tradicionalmente, una figura clave en la protección de la seguridad jurídica, garantizando la autenticidad y legalidad de los documentos a través de la certificación presencial y física de los

mismos. Sin embargo, con la irrupción de la tecnología en la era de la digitalización y la adopción de herramientas avanzadas, su rol ha evolucionado considerablemente.

El concepto de *Cyber Notar*y ha ganado relevancia en este contexto, refiriéndose a la adaptación del notario al uso de tecnologías de la información para realizar sus funciones (Aditya, Wulandari & Loso, 2022). En países como Rusia, Italia y Estonia, los avances en la digitalización notarial ya están mostrando beneficios significativos, como la reducción de tiempos de procesamiento y la mejora de la seguridad jurídica (Skachkova, Chugurova & Gubaydullina, 2020). Esta evolución implica la adopción de tecnologías como la firma electrónica y la gestión de documentos en formato digital. Estas tecnologías permiten al notario continuar su labor de validación de documentos, pero ahora en un entorno digital que demanda rapidez, eficiencia y seguridad.

El proceso tradicional de autenticar documentos mediante la presencia física de las partes ante un notario está experimentando un cambio radical. La pandemia del *COVID-19* impulsó la adopción de medidas excepcionales, como el uso de videoconferencias y la firma electrónica, para garantizar la continuidad de los servicios notariales. Sin embargo, esta transición conlleva desafíos, especialmente en lo que respecta a la seguridad y la validez de los documentos electrónicos.

En este sentido, los notarios deben adaptarse a las nuevas normativas y estándares de ciberseguridad, incluyendo el cumplimiento de leyes relacionadas por excelencia a la ciberseguridad, pero a su vez a la protección de información y transacciones electrónicas. La firma electrónica, por ejemplo, es una herramienta fundamental que permite validar la autenticidad de un documento sin necesidad de una firma física, aunque sigue existiendo el riesgo de falsificación o manipulación de datos.

A pesar de los avances, la seguridad jurídica en el entorno digital aún presenta retos. Los notarios deben adoptar medidas preventivas y contar con sistemas robustos que les permitan gestionar eficazmente los riesgos emergentes, como el robo de información, la modificación no autorizada de documentos, y los ciberataques que comprometen la integridad de los registros.

Ciberseguridad y protección de datos en las notarías

La protección de datos personales y confidenciales desde un enfoque estandarizado.

La ciberseguridad y la protección de datos personales han adquirido una relevancia crítica en las notarías debido al aumento de la digitalización y la gestión de documentos sensibles. Los notarios, como garantes de la seguridad jurídica, no solo tienen la responsabilidad de asegurar la autenticidad de los documentos físicos, sino que también deben implementar medidas tecnológicas avanzadas para proteger los datos personales y confidenciales que gestionan en formato digital.

Uno de los aspectos fundamentales es la protección de la información personalmente identificable (PII, por sus siglas en inglés), definida como cualquier dato que pueda usarse para identificar directa o indirectamente a una persona física. De acuerdo con los estándares internacionales, como la ISO/IEC 29100 y la ISO/IEC 27701, los notarios deben implementar sistemas que garanticen el manejo seguro de la PII, considerando aspectos como la minimización de datos, la retención adecuada y la prevención de accesos no autorizados.

La seguridad jurídica digital también se ve reforzada por el uso de tecnologías como la firma electrónica y la tecnología *blockchain,* las cuales permiten asegurar la autenticidad y la inmutabilidad de los documentos notariales digitales. Además, estos avances tecnológicos

deben ir acompañados de un estricto cumplimiento de las normativas de protección de datos, que incluyen la realización de evaluaciones de impacto de privacidad y la implementación de medidas de control y mitigación de riesgos ante posibles violaciones de seguridad.

En un entorno cada vez más digitalizado, las notarías también deben prestar especial atención a la clasificación de la información y a la gestión de accesos y privilegios. La clasificación adecuada de la información, basada en su nivel de sensibilidad, permite aplicar los controles de acceso necesarios para evitar el tratamiento indebido o la divulgación no autorizada de datos.

Es crucial que los notarios adopten medidas preventivas, tales como la formación continua en ciberseguridad para su personal, la actualización constante de las tecnologías utilizadas y la realización de auditorías periódicas para verificar el cumplimiento de las normativas vigentes. Esto no solo protege la información confidencial de los clientes, sino que también mitiga la responsabilidad legal en caso de brechas de seguridad.

Cumplimiento de normativas: LFPDPPP y su Reglamento.

La protección de datos personales en las notarías es un aspecto fundamental en la era digital, donde los notarios, además de ser garantes de la seguridad jurídica, deben cumplir con estrictas normativas en la materia.

Este artículo se enfoca en las funciones del notariado bajo la LFPDPPP. No se analizarán ni se tomarán en cuenta disposiciones estatales, como la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco. Dicho lo anterior, en México, el marco regulatorio clave es la LFPDPPP y su Reglamento, que establecen obligaciones claras para quienes gestionan datos personales.

La LFPDPPP y su Reglamento tienen como objetivo garantizar que el tratamiento de datos personales se realice de manera legítima, controlada e informada, salvaguardando los derechos de privacidad y autodeterminación informativa de los individuos. Los notarios, al manejar información confidencial y sensible, deben adoptar medidas técnicas, físicas y administrativas para proteger los datos que procesan, tal como lo establece la Ley y las disposiciones sobre seguridad en su Reglamento.

Los notarios deben adherirse a los principios fundamentales de protección de datos establecidos en la LFPDPPP, tales como la licitud, consentimiento, calidad de los datos, confidencialidad y seguridad. Asimismo, deben garantizar que los datos personales sean tratados de acuerdo con las finalidades específicas, explícitas y legítimas por las cuales fueron recabados, y no utilizados para fines distintos sin el consentimiento del titular.

El Reglamento de la LFPDPPP exige a los responsables implementar medidas de seguridad para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso no autorizado. Esto incluye el uso de tecnologías seguras como la firma electrónica y la tecnología *blockchain,* que aseguran la integridad y autenticidad de los documentos notariales.

En caso de incumplimiento de la LFPDPPP, los notarios pueden enfrentar sanciones administrativas y legales. Las infracciones van desde multas hasta la posibilidad de responsabilidades penales en situaciones de tratamiento indebido o filtraciones de datos personales.

Este apartado resalta la importancia de que los notarios no solo deben garantizar la validez jurídica de los actos que autorizan, sino también la protección adecuada de los datos personales conforme a la normativa

vigente, previniendo posibles riesgos asociados a la digitalización de los servicios notariales.

Responsabilidad del notario en caso de brechas de seguridad.

Las notarías, como instituciones clave en la gestión de documentos y transacciones legales, tienen acceso a una cantidad significativa de información personal y confidencial, lo que las convierte en blancos sensibles de incidentes de seguridad cibernética. Dado el manejo de datos personales de alta relevancia, como información patrimonial, testamentos, poderes notariales y contratos, los notarios tienen la obligación legal de garantizar la protección de estos datos frente a cualquier amenaza que pueda comprometer su confidencialidad, integridad o disponibilidad.

En México, la LFPDPPP y su Reglamento imponen a los responsables del tratamiento de datos, entre ellos los notarios, el deber de implementar medidas de seguridad físicas, técnicas y administrativas adecuadas para prevenir cualquier vulneración de la información personal. Estas obligaciones no solo están diseñadas para proteger los derechos patrimoniales de los titulares, sino también sus derechos incorpóreos, que pueden incluir el derecho al honor, la reputación y la privacidad.

Una vulneración a la seguridad de los datos personales, definida como cualquier incidente que comprometa la confidencialidad, integridad o disponibilidad de la información, puede tener consecuencias significativas para el notario en términos legales, reputacionales y operativos. De acuerdo con el artículo 20 de la LFPDPPP, el artículo 63 de su Reglamento, y las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los notarios tienen el deber de actuar rápidamente ante cualquier incidente de seguridad que afecte los datos personales bajo su custodia.

En caso de que ocurra una brecha de seguridad, el notario debe cumplir con diversas responsabilidades. La primera es la identificación inmediata del incidente, siguiendo un plan de respuesta a incidentes de seguridad que debe estar previamente elaborado y alineado con estándares internacionales de seguridad, como los desarrollados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

El plan de respuesta a incidentes debe incluir, al menos, las siguientes fases (INAI, 2018):

- **Preparación:** El notario debe haber implementado políticas y controles que permitan la rápida detección de incidentes de seguridad. Esto implica la capacitación continua de su personal, la instalación de sistemas de monitoreo de seguridad, como *firewalls* y sistemas de detección de intrusos, y la realización de copias de seguridad periódicas para minimizar el impacto de cualquier pérdida de datos.

- **Identificación:** Una vez detectada una alerta de seguridad, el notario debe identificar si se trata de un incidente real que involucre la seguridad de los datos personales. Esta fase incluye la documentación detallada del incidente, describiendo cómo y cuándo ocurrió, qué sistemas de tratamiento fueron comprometidos, y qué datos personales se vieron afectados.

- **Contención:** Una vez identificado el incidente, el notario debe proceder a contener el problema, limitando el impacto en los sistemas y activos comprometidos. Si el incidente afecta medios de almacenamiento electrónico, como bases de datos o sistemas informáticos, se deben aislar los equipos comprometidos para evitar la propagación de la brecha.

- **Mitigación:** Esta etapa implica tomar medidas correctivas para minimizar los efectos del incidente y prevenir que se repita en el futuro. Esto puede incluir la instalación de nuevas medidas de seguridad, la actualización de sistemas y la eliminación de vulnerabilidades que fueron explotadas durante la brecha.

- **Recuperación:** Una vez mitigado el incidente, el notario debe asegurarse de que los sistemas afectados regresen a su funcionamiento normal. Durante esta fase, es vital realizar un monitoreo constante para asegurar que las nuevas medidas de seguridad implementadas sean efectivas y no generen fallas adicionales.

- **Mejora continua:** Tras resolver el incidente, el notario debe documentar todas las acciones realizadas y comunicar las lecciones aprendidas al personal involucrado, asegurando una mejora constante de las medidas de seguridad. Este aprendizaje servirá para fortalecer la capacidad de respuesta ante futuros incidentes.

Una de las obligaciones más importantes del notario en caso de una brecha de seguridad es la notificación oportuna tanto a los titulares de los datos afectados como, en su caso, a las autoridades competentes. De acuerdo con la normativa aplicable, el notario tiene un plazo de hasta 72 horas para informar a los titulares sobre la naturaleza del incidente, los datos comprometidos y las medidas correctivas adoptadas. Además, debe proporcionar recomendaciones para que los titulares puedan protegerse ante posibles afectaciones derivadas del incidente, como en casos de robo de identidad.

Para la notificación a los titulares, se recomienda un enfoque directo, utilizando canales de comunicación como el correo electrónico o el teléfono, asegurando que la información sea clara, precisa y que no contenga detalles técnicos innecesarios que puedan generar confusión. Asimismo, en casos graves que impliquen una afectación significativa a

los derechos de los titulares, de manera indicativa, es necesario notificar a las autoridades, como el INAI, proporcionando detalles sobre las medidas adoptadas para mitigar el impacto del incidente.

El incumplimiento de las obligaciones de protección de datos por parte del notario puede resultar en severas sanciones, que incluyen multas impuestas por el INAI, las cuales pueden ser atenuadas si el notario demuestra haber implementado medidas correctivas y haber notificado a las autoridades y a los titulares de manera oportuna. Adicionalmente, el notario puede enfrentar repercusiones legales en caso de que se determine que la brecha de seguridad fue resultado de negligencia o falta de diligencia en la implementación de medidas de seguridad.

En un entorno donde las amenazas cibernéticas están en constante evolución, es esencial que los notarios no solo cumplan con la normativa de protección de datos, sino que adopten una postura proactiva en cuanto a la seguridad de la información. Esto implica la inversión en tecnologías de protección, como sistemas de encriptación y monitoreo, la actualización constante de las políticas de seguridad, y la formación continua del personal en buenas prácticas de ciberseguridad.

Las notarías, al igual que otras entidades que manejan datos sensibles, deben estar preparadas para enfrentar los retos de la era digital. Una adecuada gestión de la seguridad de la información no solo protege a los titulares de datos personales, sino que también preserva la integridad y reputación del notario, garantizando la confianza de sus clientes y la continuidad de sus operaciones.

Implementación de tecnologías digitales en el ámbito notarial

Firma electrónica: Tipos y su validez legal.

La digitalización en el ámbito notarial no solo ha mejorado la eficiencia de los trámites, sino que también ha puesto de manifiesto la importancia de la ciberseguridad en la protección de los datos sensibles y la integridad de los documentos notariales. Uno de los componentes críticos de esta transformación es la adopción de la firma electrónica, la cual, en un contexto digital, se enfrenta a retos importantes relacionados con la protección contra ciberataques y la prevención de fraudes.

La Firma Electrónica Simple, aunque útil en ciertos trámites menores, carece de las medidas de seguridad robustas que aseguren la identidad del firmante de manera inequívoca. Desde una perspectiva de ciberseguridad, la firma electrónica simple es más vulnerable a la suplantación de identidad y a los ataques de tipo *"man-in-the-middle"* (interceptación de datos), lo que la hace menos adecuada para actos notariales de alto valor legal.

Por otra parte, la Firma Electrónica Avanzada o Certificada regulada por la Ley de Firma Electrónica Certificada del Estado de Jalisco, implica un mayor nivel de seguridad, al estar respaldada por certificados digitales emitidos por autoridades certificadoras reconocidas. Este tipo de firma asegura la autenticidad y la integridad de los documentos mediante tecnologías criptográficas. De esta forma, se minimizan los riesgos de fraude o manipulación de datos, dos de los principales desafíos en ciberseguridad en entornos digitales.

La firma electrónica avanzada, además de tener plena validez legal, ofrece garantías de confidencialidad y protección contra accesos no autorizados. Para los notarios, el uso de estas tecnologías requiere la implementación de plataformas seguras y certificadas que protejan los

documentos contra ataques cibernéticos. Asimismo, es fundamental que se implementen medidas como la encriptación de los documentos y el uso de redes seguras para la transmisión de datos entre las partes involucradas. Según la Ley de Notariado del Estado de Jalisco como fundamento habilitante y el Reglamento de la Ley del Notariado en Materia de Duplicados y Avisos Notariales Electrónicos, los documentos firmados electrónicamente deben ser conservados de manera segura, evitando cualquier alteración no autorizada.

El incremento en el uso de la firma electrónica avanzada plantea nuevos retos para los notarios, quienes deben asegurarse de cumplir con los estándares más altos de ciberseguridad. Esto incluye la actualización constante de los sistemas de seguridad para prevenir ataques como el *phishing*, la suplantación de identidad, o el robo de datos. Además, los notarios deben trabajar en estrecha colaboración con autoridades de certificación y plataformas tecnológicas para garantizar que los protocolos de seguridad cumplan con las normativas vigentes y las mejores prácticas en ciberseguridad.

Uso de *blockchain* para la certificación de documentos.

La ciberseguridad ha cobrado una relevancia primordial en el ámbito notarial, especialmente con la adopción de nuevas tecnologías digitales como *blockchain*. Esta tecnología, que se basa en una red descentralizada y utiliza la criptografía para proteger la información, se presenta como una herramienta ideal para la certificación y validación de documentos notariales, ofreciendo una solución robusta contra los riesgos asociados a la falsificación y manipulación de documentos.

Blockchain permite crear un registro inmutable y distribuido, donde cada transacción (o documento) es validada y almacenada en un bloque que, a su vez, se conecta de manera criptográfica con el bloque anterior. Esto asegura que cualquier intento de modificar un documento previo

quede registrado y sea fácilmente detectable, garantizando así la integridad y la autenticidad del documento certificado.

En el ámbito notarial, la tecnología *blockchain* se puede utilizar para (Prusty, 2018):

- **Certificación de autenticidad:** A través del uso de contratos inteligentes *(smart contracts)*, el notario puede garantizar que los documentos digitales no han sido alterados después de su creación y firma.

- **Registro inmutable**: Los documentos certificados se almacenan en la cadena de bloques, lo que significa que cualquier alteración en ellos generaría discrepancias detectables de inmediato. Esto elimina el riesgo de fraude documental.

- **Trazabilidad:** *Blockchain* ofrece un historial claro de quién creó, modificó o accedió a un documento, proporcionando un registro auditado de las interacciones que han tenido lugar con el documento, lo que resulta útil en auditorías y disputas legales.

La implementación de la tecnología *blockchain* también refuerza la seguridad en la certificación de documentos notariales. Cada documento registrado en la cadena de bloques está protegido mediante algoritmos criptográficos avanzados, lo que reduce considerablemente el riesgo de accesos no autorizados o manipulaciones. Además, la naturaleza distribuida de la tecnología *blockchain* elimina la dependencia de un único punto de fallo, un problema típico de los sistemas centralizados.

Las aplicaciones *blockchain* en el ámbito notarial incluyen (Prusty, 2018):

- **Control de acceso:** Solo los usuarios autorizados, como los notarios y las partes interesadas, pueden acceder y verificar los documentos mediante sistemas de claves públicas y privadas.

- **Validación distribuida:** En lugar de depender de un sistema centralizado para validar la autenticidad de un documento, la red de nodos del blockchain realiza una verificación descentralizada, eliminando así los riesgos de manipulación interna o externa.

A pesar de las ventajas de la tecnología blockchain, su implementación también plantea desafíos en términos de interoperabilidad con los sistemas actuales y de la necesidad de que los notarios y otras partes involucradas estén debidamente capacitados para manejar y operar estas nuevas tecnologías. Además, es esencial garantizar el cumplimiento de las regulaciones vigentes, como las leyes de protección de datos y la normativa notarial.

Riesgos emergentes en la ciberseguridad para notarías

Amenazas cibernéticas en la gestión de documentos notariales.

En el contexto actual, las notarías enfrentan una serie de riesgos cibernéticos emergentes debido a la creciente digitalización de los procesos notariales y la gestión de documentos electrónicos. Estas amenazas se centran principalmente en la protección de la información sensible y confidencial, lo que convierte a las notarías en un objetivo atractivo para los ciberdelincuentes.

Uno de los riesgos más significativos es la filtración de documentos notariales a través de ataques de *phishing* y *ransomware*. Estas técnicas son utilizadas para acceder a los sistemas notariales, lo que podría resultar en el robo, alteración o eliminación de documentos críticos, como contratos, escrituras y poderes. El *ransomware,* en particular, ha evolucionado y ya

no solo busca el cifrado de archivos, sino también la exfiltración de datos para presionar a las víctimas mediante la doble extorsión.

Además, las vulnerabilidades en el *software* utilizado para la gestión de documentos representan otro riesgo importante. Los sistemas que no han sido actualizados regularmente pueden contener vulnerabilidades no parcheadas, que permiten a los atacantes comprometer los sistemas a través de *exploits* conocidos. Esto puede derivar en la pérdida de integridad y confidencialidad de los documentos notariales.

Por otro lado, las configuraciones incorrectas de seguridad en los sistemas de gestión documental, como contraseñas débiles o el mal manejo de permisos de acceso, pueden abrir la puerta a amenazas internas y errores humanos, lo que facilita el acceso no autorizado a los documentos o la manipulación indebida de los mismos.

Finalmente, los dispositivos no asegurados dentro de la infraestructura de la notaría, como las computadoras personales o dispositivos móviles utilizados para acceder a los sistemas, incrementan el riesgo de brechas de seguridad. Estos dispositivos pueden ser blanco fácil de ataques de *malware* si no cuentan con una adecuada gestión de seguridad.

En conclusión, las notarías deben adoptar una estrategia integral de ciberseguridad que incluya la protección contra vulnerabilidades, la educación en buenas prácticas de seguridad, y el uso de autenticación multifactor para mitigar estos riesgos y salvaguardar la confidencialidad e integridad de los documentos notariales.

Fraude digital y suplantación de identidad.

La transformación digital en las notarías ha facilitado la gestión y almacenamiento de documentos, pero también ha incrementado la exposición a riesgos cibernéticos, particularmente en lo que respecta al

fraude digital y la suplantación de identidad. Estos riesgos no solo afectan la confianza de los clientes, sino que pueden tener graves implicaciones legales y económicas tanto para las notarías como para sus usuarios.

El fraude digital en notarías puede ocurrir cuando ciberdelincuentes logran acceder a los sistemas notariales mediante técnicas de ingeniería social, como *phishing* o ataques de malware, lo que les permite alterar o falsificar documentos notariales electrónicos. Estos ataques pueden comprometer la integridad de la información notarial, llevando a la emisión de certificados o contratos fraudulentos que podrían ser difíciles de detectar sin los mecanismos de autenticación adecuados, como la firma digital o autenticación multifactor.

Por otro lado, la suplantación de identidad representa una amenaza importante, ya que los atacantes pueden utilizar información robada para hacerse pasar por clientes legítimos o incluso por los propios notarios. La suplantación puede permitir la ejecución de transacciones o la firma de documentos sin el conocimiento o consentimiento de las partes involucradas. La legislación en muchos países aún está evolucionando para enfrentar estas amenazas de manera efectiva, y en algunos casos, los ataques de identidad digital facilitan otros delitos más graves como el fraude económico o la evasión de responsabilidades legales.

Para combatir estas amenazas, es imperativo que las notarías implementen mecanismos avanzados de autenticación y adopten políticas de ciberseguridad robustas. Esto incluye la constante vigilancia de los accesos a los sistemas notariales, la educación del personal sobre las técnicas de fraude más comunes, y la adopción de medidas tecnológicas que garanticen la protección de la identidad y la información sensible en los documentos que gestionan.

Mejores prácticas en ciberseguridad para notarías

Hacia un Sistema de gestión de la seguridad de la información.

En el contexto actual, donde las notarías manejan información altamente sensible, es esencial adoptar un enfoque estructurado para la gestión de la seguridad de la información. El estándar ISO/IEC 27001:2022 proporciona un marco robusto para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). A continuación, se describen las mejores prácticas clave que las notarías pueden adoptar.

La implementación de un SGSI comienza con una evaluación integral de los riesgos. Las notarías deben identificar y evaluar los riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad de la información. Este proceso debe considerar tanto factores internos como externos, incluyendo amenazas cibernéticas y la naturaleza del entorno legal en el que operan.

Las notarías deben definir una política clara de seguridad de la información que esté alineada con sus objetivos estratégicos y que sea comunicada a todo el personal. Esta política debe incluir objetivos específicos de seguridad, compromisos con el cumplimiento normativo y el compromiso con la mejora continua del sistema de seguridad.

Es vital que las notarías clasifiquen la información que manejan según su nivel de sensibilidad. Esto permitirá establecer controles de acceso adecuados, garantizando que solo las personas autorizadas puedan acceder a información confidencial. La autenticación robusta y la segregación de funciones son esenciales para prevenir el acceso no autorizado.

Las notarías deben estar preparadas para responder eficazmente a incidentes de seguridad, tales como intentos de acceso no autorizado o violaciones de datos. El desarrollo de un plan de gestión de incidentes, que incluya la recolección de evidencia y la notificación a las partes interesadas, es fundamental para mitigar los daños y prevenir futuros incidentes.

El personal de las notarías, incluidos los empleados y terceros relacionados, debe recibir formación regular en ciberseguridad. Esto no solo refuerza el cumplimiento de las políticas de seguridad, sino que también incrementa la conciencia sobre la importancia de proteger la información contra amenazas cibernéticas y errores humanos.

Dado que muchas notarías dependen de sistemas tecnológicos para almacenar y gestionar la información, es importante garantizar que estos sistemas estén debidamente asegurados. Asimismo, cualquier relación con proveedores tecnológicos debe incluir cláusulas de seguridad en los contratos, asegurando que estos también cumplan con las normativas de protección de la información.

Finalmente, un SGSI debe ser revisado y actualizado continuamente para adaptarse a los cambios tecnológicos, las nuevas normativas y las lecciones aprendidas de incidentes previos. Las auditorías internas y externas son herramientas clave para garantizar que el sistema sigue siendo eficaz y se ajusta a los requisitos normativos aplicables.

La implementación de estas prácticas no solo refuerza la seguridad de la información en las notarías, sino que también genera confianza entre los clientes y las autoridades, asegurando que se respeten los principios de confidencialidad, integridad y disponibilidad de la información que manejan.

Controles y mejores prácticas para luchar contra el ciber riesgo.

El aumento de las amenazas cibernéticas, tales como el robo de identidad, el acceso no autorizado y la manipulación de documentos sensibles, ha generado la necesidad de que las notarías adopten medidas de ciberseguridad avanzadas. Al ser guardianes de documentos críticos y datos personales, las notarías deben implementar un conjunto integral de controles y mejores prácticas basadas, verbigracia, en el estándar ISO/IEC 27002:2022 para proteger su información.

Las notarías deben establecer políticas estrictas de control de acceso para garantizar que solo las personas autorizadas tengan acceso a la información crítica. Esto incluye la implementación de sistemas de autenticación multifactor (MFA) y la gestión adecuada de credenciales. Los privilegios de acceso deben revisarse periódicamente para evitar la acumulación innecesaria de permisos.

Es determinante que las notarías implementen soluciones de protección contra *malware,* tales como antivirus y *software antimalware*, y aseguren su constante actualización. Además, deben gestionar las vulnerabilidades identificadas en los sistemas mediante la aplicación de parches de seguridad y la actualización continua de los sistemas de *software* utilizados.

El uso de redes seguras es esencial para prevenir accesos no autorizados. Esto incluye la segmentación de redes, la utilización de *firewalls* y sistemas de detección y prevención de intrusiones (IDS/IPS). La monitorización de la red en tiempo real también ayuda a detectar posibles ataques antes de que puedan causar daños significativos.

Las notarías manejan grandes cantidades de información clasificada que debe ser protegida conforme a su nivel de confidencialidad. La información debe clasificarse según su sensibilidad, y las medidas de

protección deben estar alineadas con esta clasificación, asegurando que los datos más sensibles estén encriptados tanto en reposo como en tránsito.

Ante la creciente amenaza de ataques cibernéticos, las notarías deben desarrollar y mantener un plan de gestión de incidentes de seguridad que les permita reaccionar de manera rápida y eficiente. Esto incluye la detección temprana de incidentes, la recolección de pruebas y la notificación a las autoridades pertinentes. Aprender de incidentes pasados también es fundamental para mejorar continuamente la respuesta a amenazas.

Dado que los empleados son uno de los principales vectores de ciber riesgo, la capacitación continua en prácticas de seguridad de la información es esencial. Los empleados deben estar familiarizados con las políticas de ciberseguridad y recibir formación periódica para identificar amenazas, como ataques de *phishing*, y aplicar las mejores prácticas en su trabajo diario.

Las notarías deben asegurarse de que toda la información confidencial sea encriptada tanto en tránsito como en reposo. El uso de criptografía robusta no solo protege la confidencialidad de los datos, sino que también garantiza la integridad y disponibilidad de la información durante su transferencia.

Finalmente, es vital que las notarías realicen auditorías periódicas de sus sistemas de seguridad para asegurar que las medidas implementadas siguen siendo efectivas frente a las nuevas amenazas cibernéticas. Estas auditorías también permiten la identificación de áreas de mejora y garantizan el cumplimiento de las normativas aplicables.

Conclusiones

La evolución del rol del notario en la era digital plantea importantes desafíos y oportunidades en el ámbito de la ciberseguridad. Si bien la función tradicional del notario ha sido asegurar la autenticidad y validez de los documentos a través de procesos presenciales, la adopción de tecnologías como la firma electrónica, la *blockchain* y la gestión digital de documentos ha transformado esta función, exigiendo una mayor atención a la protección de datos y la seguridad cibernética.

El concepto del *Cyber Notary* o notario cibernético, refleja esta transición hacia un entorno digital, donde los notarios deben no solo garantizar la seguridad jurídica, sino también implementar medidas tecnológicas avanzadas que protejan la información personal y confidencial. La adopción de tecnologías como la firma electrónica avanzada y *blockchain* ofrece nuevas formas de certificar documentos de manera segura, aunque no sin riesgos. La suplantación de identidad, el fraude digital y las brechas de seguridad son amenazas reales que exigen la adopción de políticas robustas de ciberseguridad y el cumplimiento de normativas como la LFPDPPP, y su Reglamento, así como las normatividades estatales en la materia.

A lo largo de este análisis, se ha destacado la importancia de que los notarios implementen sistemas de gestión de la seguridad de la información, sigan las mejores prácticas internacionales, y adopten una postura proactiva frente a los riesgos emergentes. Esto implica no solo la capacitación continua de su personal y la actualización de sus tecnologías, sino también la ejecución de auditorías periódicas y la aplicación rigurosa de medidas preventivas para mitigar los ciber riesgos.

En conclusión, el notariado en la era digital debe ser capaz de integrar la ciberseguridad como un componente esencial de su actividad diaria, garantizando que la protección de la información confidencial y la

integridad de los documentos siga siendo la piedra angular de su función. Esto no solo asegura la confianza del público en los servicios notariales, sino que también refuerza la seguridad jurídica en un entorno cada vez más digitalizado y expuesto a riesgos cibernéticos.

Referencias

- Aditya, A., Wulandari, C., & Loso, L. (2022). Cyber Notary: Between Notary Opportunities And Challenges In Facing The Era Of Digital Disruption 4.0 Towards 5.0. International Journal of Law Society Services, 2(1), 8-15.

- INAI. (2018). Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales. Editorial Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.

- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and

- ISO/IEC 27002 for privacy information management — Requirements and guidelines.

- ISO/IEC 29100:2024 Information technology — Security techniques — Privacy framework.

- Ley de Firma Electrónica Certificada del Estado de Jalisco y sus Municipios. Periódico Oficial del Estado de Jalisco. Decreto No. 24459/LVII/06. 2006.

- Ley del Notariado del Estado de Jalisco. Periódico Oficial del Estado de Jalisco. Decreto No. 21459/LVII/06. 2006.

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, DOF, 5 de julio de 2010.

- Prusty, N. (2018). Blockchain for Enterprise: Build scalable blockchain applications with privacy, interoperability, and permissioned features. Packt Publishing Ltd.

- Reglamento de la Ley del Notariado del Estado de Jalisco en Materia de Duplicados y Avisos Notariales Electrónicos. Periódico Oficial del Estado de Jalisco. DIGELAG ACU 046/2011. 2011.

- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, DOF, 21 de diciembre de 2011.

- Skachkova, O. S., Chugurova, T. V., & Gubaydullina, E. K. (2020). Digital Notary As A Necessary Element Of Digital Economy: International Experience. In S. I. Ashmarina, & V. V. Mantulenko (Eds.), Global Challenges and Prospects of the Modern Economic Development, vol 79. European Proceedings of Social and Behavioural Sciences (pp. 360-366). European Publisher.