

COMISIÓN:
Informática

TEMA:

“Ciberseguridad en Estudios Jurídicos”

**La ciberseguridad en el ejercicio de la abogacía:
Riesgos, responsabilidad y protección profesional**

SUBTEMAS:

1. Incorporación de medidas de ciberseguridad en los Códigos de Ética Profesional
2. Herramientas y prácticas de bajo costo para estudios jurídicos
3. Autenticación multifactor (MFA) y protección de expedientes digitales
4. Capacitación continua en ciberseguridad aplicada a la abogacía
5. Protocolo de respuesta ante incidentes de seguridad informática

AUTOR:
Ezequiel Walter Rodríguez

INSCRIPCIÓN PROFESIONAL:
Colegio de Abogados de La Matanza (CALM)

DOMICILIO:
Entre Ríos 2942 PB, San Justo, Provincia de Buenos Aires, Argentina

TELÉFONO:
113.424.3684

CORREO ELECTRÓNICO:
ezequielwrodriguez@gmail.com

La ciberseguridad en el ejercicio de la abogacía: Riesgos, responsabilidad y protección profesional

Abstract

El presente trabajo aborda la importancia crítica de la ciberseguridad en el ejercicio de la abogacía, considerando los riesgos éticos y legales derivados de la creciente digitalización de los expedientes y comunicaciones electrónicas en la Provincia de Buenos Aires. Se propone la incorporación de prácticas de ciberseguridad en los códigos de ética profesional, imponiendo la obligación de implementar medidas tecnológicas que protejan la información sensible de los clientes y preserven la confidencialidad. Asimismo, se subraya la necesidad de que los abogados reciban formación continua en esta área para mantenerse actualizados frente a amenazas cibernéticas emergentes, evitando negligencias profesionales que puedan traducirse en sanciones legales. Se analizan, además, recomendaciones prácticas que incluyen el uso de herramientas de bajo costo, protocolos internos de seguridad y la adopción de tecnologías como el cifrado y la autenticación multifactor, elementos esenciales para garantizar un entorno digital seguro. Este enfoque integral busca consolidar la ciberseguridad como un deber ético ineludible, asegurando el ejercicio responsable de la profesión y la protección de los intereses de los clientes en la era digital.

Introducción

En el contexto actual de creciente digitalización de los procesos judiciales y las comunicaciones profesionales, el ejercicio de la abogacía enfrenta nuevos desafíos en materia de ciberseguridad. La confidencialidad de la información y la integridad de los datos sensibles se ven comprometidas por el aumento exponencial de amenazas cibernéticas, tales como el ransomware, el phishing dirigido y las brechas de seguridad en infraestructuras tecnológicas. Este escenario impone a los abogados la obligación ineludible de adoptar medidas técnicas que garanticen la protección de los datos y la seguridad de las comunicaciones, conforme a lo establecido en la normativa vigente.

El presente análisis se enfoca en la necesidad de integrar la ciberseguridad dentro de los marcos éticos y profesionales de la abogacía, proponiendo su incorporación en los códigos de conducta de los colegios de abogados y destacando la formación continua como elemento fundamental para mitigar riesgos tecnológicos. Al mismo tiempo, se identifican herramientas y estrategias de bajo costo que pueden ser implementadas de manera efectiva en los estudios jurídicos, consolidando así un enfoque proactivo y preventivo frente a las vulnerabilidades informáticas. La implementación de estas prácticas no solo protege la confidencialidad de los expedientes, sino

que refuerza la confianza del cliente y la integridad del abogado en un entorno digital cada vez más expuesto a riesgos.

I.-

En el marco de la creciente digitalización de los expedientes judiciales y la dependencia de recursos tecnológicos, los abogados deben adoptar un enfoque proactivo en materia de ciberseguridad. La responsabilidad derivada de la protección de información confidencial, tanto personal como legal, impone la obligación de implementar medidas rigurosas que prevengan vulnerabilidades tecnológicas. Los abogados manejan una gran cantidad de información sensible, incluyendo datos personales, secretos comerciales y estrategias legales. Esta información es un objetivo atractivo para ciberdelincuentes que buscan obtener una ventaja competitiva, extorsionar a las víctimas o simplemente causar daños.

Estos ataques pueden tener consecuencias graves para los abogados y sus clientes, incluyendo:

Pérdida de datos confidenciales: Exposición de información sensible que puede ser utilizada para cometer fraudes, extorsionar o dañar la reputación del cliente. (ley 25.326)

Interrupción de los servicios: Imposibilidad de acceder a los sistemas informáticos, lo que puede paralizar las operaciones del estudio jurídico.

Multas y sanciones: Incumplimiento de las regulaciones de protección de datos, lo que puede resultar en sanciones económicas y daños a la reputación. Por ejemplo, incumplir el deber de confidencialidad y seguridad sobre los datos personales incorporados en una base de datos; mantener bases de datos locales, programas o equipos que contengan datos personales sin las debidas condiciones de seguridad que la normativa determina;

(ley 25.326)

Daños a la reputación: Pérdida de confianza de los clientes y daños a la imagen profesional del abogado.

Responsabilidad legal: Posibilidad de ser demandado por los clientes afectados por una brecha de seguridad.

La ciberseguridad es un aspecto fundamental del ejercicio de la abogacía en la era digital. Los abogados deben adoptar estrategias de seguridad para proteger la información confidencial de sus clientes y garantizar la continuidad de sus operaciones. Al implementar las medidas de seguridad,

los abogados pueden reducir significativamente el riesgo de sufrir un ciberataque y proteger su reputación profesional.

Las consecuencias de no contar con medidas de protección adecuadas comprometen la integridad de los expedientes y la exposición de información confidencial puede afectar la estrategia legal que se haya elaborado.

Un punto que deben comenzar a tener en cuenta son las potenciales sanciones por incumplir normas de protección de datos (Ley 25.326 de Protección de Datos Personales) y la posible responsabilidad penal o civil en caso de daños a terceros.

II. La relación entre la ciberseguridad y la responsabilidad profesional

El deber de confidencialidad y secreto profesional

El artículo 156 del Código Penal argentino establece penas para quien, por su estado, profesión o función, divulgue secretos que se le hayan confiado en razón de su ejercicio. Este deber se extiende a los entornos digitales. El abogado tiene la obligación de proteger no solo la información física, sino también la digital, especialmente con la creciente digitalización de expedientes en la Provincia de Buenos Aires.

Responsabilidad ética y disciplinaria en el ámbito digital

El incumplimiento de los estándares de ciberseguridad puede ser considerado una falta ética grave, que compromete el ejercicio responsable de la profesión.

Los colegios de abogados, tanto en el ámbito nacional como en la Provincia de Buenos Aires, deberán, en la brevedad, comenzar a incorporar sanciones más estrictas para quienes no tomen medidas adecuadas de protección digital.

La normativa local de la Suprema Corte de Justicia de Buenos Aires, que establece la digitalización de los expedientes judiciales y su implicancia en la seguridad de estos.

Los abogados que no implementen medidas adecuadas pueden ser responsables por daños causados a sus clientes si la falta de protección permite la exposición de datos confidenciales y quedar expuestos a potenciales acciones de responsabilidad civil por negligencia profesional derivadas de ciberataques.

Implicaciones en el seguro de responsabilidad profesional

Es posible que las aseguradoras revisen las pólizas de responsabilidad profesional de los abogados, exigiendo que se cumplan con estándares mínimos de ciberseguridad para otorgar cobertura frente a incidentes de ciberseguridad.

La ciberseguridad no es un tema ajeno al ejercicio de la abogacía, especialmente en la Provincia de Buenos Aires, donde la digitalización de los expedientes y las comunicaciones entre abogados y clientes es cada vez más común. La falta de implementación de medidas adecuadas no solo expone al abogado a riesgos éticos, sino también a sanciones legales. Es crucial que los abogados adopten una postura proactiva frente a estos desafíos, protegiendo tanto su ejercicio profesional como los intereses de sus clientes.

Ahora veamos algunos de los riesgos cibernéticos en el ámbito legal al cual se expone la abogacía. Las ciberamenazas más comunes que enfrentan los abogados:

1.- Phishing y spear-phishing:

Estos ataques son intentos de suplantación de identidad que buscan robar credenciales de acceso o comprometer redes internas. Los ciberdelincuentes utilizan correos electrónicos falsificados que imitan comunicaciones legítimas. En el spear-phishing, el atacante estudia detalladamente a la víctima, haciendo que los correos maliciosos parezcan genuinos.

Técnica de mitigación: Implementar sistemas de detección de phishing basados en inteligencia artificial que analicen patrones inusuales en las comunicaciones.

2. Ransomware:

Este tipo de malware cifra los archivos en el sistema del abogado y solicita un rescate para liberarlos. Los estudios jurídicos son objetivos prioritarios, ya que manejan información valiosa. El ransomware puede propagarse a través de correos electrónicos, descargas comprometidas o vulnerabilidades en los sistemas operativos.

Técnica de mitigación: Emplear software de protección de endpoint con capacidades de respuesta automatizada para detener la propagación de malware y mantener backups fuera de línea con versiones previas no comprometidas.

3. Ataques de intermediarios (Man-in-the-middle):

Este ataque permite a los delincuentes interceptar y manipular la comunicación entre el abogado y su cliente o un tercero, sin que ninguna de las partes lo detecte.

Técnica de mitigación: Utilización de protocolos de encriptación de extremo a extremo en correos electrónicos y mensajería, como PGP (Pretty Good Privacy) y certificados TLS robustos en sitios web y servicios en línea.

Vulnerabilidades en sistemas de gestión documental

Muchas firmas legales utilizan software especializado para administrar expedientes digitales ejemplo de ellos son DretLaw Link: <http://www.dretlaw.com.ar>; Legal Soft Link: <http://legalsoft.com.ar>; y, tal vez, el mas conocido el LEX DOXTOR.

Si sus softwares no se actualizan regularmente, estos sistemas pueden tener vulnerabilidades que un atacante puede explotar para obtener acceso no autorizado.

Técnica de mitigación: Implementación de un sistema de parches automatizados y verificación periódica de vulnerabilidades con herramientas de análisis de seguridad, como escáneres de vulnerabilidades (p. ej., OpenVAS, Nessus).

Los sistemas no seguros permiten que los ciberdelincuentes accedan a documentos legales, correspondencia privilegiada y datos sensibles de los clientes. Esta exposición puede comprometer casos en curso o generar un daño irreparable a la reputación de los clientes y del propio abogado.

III.- Responsabilidad ética y disciplinaria en el ámbito digital

Fallas en ciberseguridad como negligencia profesional

El desconocimiento o la falta de implementación de medidas de seguridad puede ser considerado una falta ética grave. Los colegios de abogados podrían sancionar a aquellos profesionales que no tomen medidas de ciberseguridad, considerándolo como una violación de la ética y del deber de diligencia.

Ley de Protección de Datos Personales (Ley 25.326) obliga a los estudios jurídicos a implementar medidas técnicas para garantizar la seguridad de los datos personales que procesan. Esto incluye la adopción de procedimientos de seguridad informática y la notificación en caso de brechas de datos.

Suprema Corte de Justicia de Buenos Aires, por su parte ha implementado una serie de directrices respecto de la digitalización de expedientes judiciales, lo que exige a los abogados garantizar la seguridad en el manejo de los mismos. Esto implica el uso de plataformas seguras para la presentación y almacenamiento de documentos judiciales.

Responsabilidad penal por la divulgación de información sensible, el abogado como víctima de estos delitos informáticos.

La divulgación no autorizada de información confidencial puede configurar diversos delitos penales, según la gravedad de la conducta y las circunstancias del caso.

Algunos de los delitos más comunes incluyen:

Acceso indebido a un sistema informático (art. 153 del Código Penal): El acceso a sistemas informáticos sin autorización, con el fin de obtener información confidencial, puede ser sancionado con prisión.

Interceptación de comunicaciones (art. 159 del Código Penal): La interceptación de comunicaciones electrónicas, como correos electrónicos o mensajes instantáneos, puede constituir un delito penal.

Violación de secretos (art. 157 del Código Penal): La revelación de secretos, como los contenidos de expedientes judiciales, puede ser sancionada penalmente.

Ahora cabe preguntarse si la falta de cuidado o protección podría derivar en sanciones penales o si el abogado pudiera ser objeto de acciones disciplinarias por parte del Colegio de Abogados, lo que podría derivar en la suspensión o revocación de su matrícula.

IV.- Recomendaciones prácticas para estudios jurídicos

Checklist de seguridad para estudios jurídicos

A continuación, se presenta una lista de verificación básica de ciberseguridad que todo estudio jurídico debería implementar para reducir el riesgo de ataques cibernéticos y cumplir con los estándares de protección de datos.

Gestión de contraseñas:

Utilizar contraseñas seguras y únicas para cada cuenta.

Gestión segura de contraseñas: se deben usar gestores de contraseñas y activar el doble factor de autenticación (2FA) para el acceso a todos sus sistemas críticos. Las contraseñas deben cumplir con requisitos de complejidad (mínimo de 12 caracteres con una combinación de letras, números y símbolos).

Almacenar contraseñas en un gestor de contraseñas seguro (p. ej., Bitwarden, LastPass).

Protección de dispositivos:

Instalar software antivirus y antimalware en todos los dispositivos.

Habilitar la encriptación de disco completo (Full Disk Encryption) en computadoras y dispositivos móviles.

Mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad.

Copia de seguridad (backup):

Realizar copias de seguridad automáticas y regulares de todos los expedientes críticos, almacenándolos en ubicaciones seguras y fuera de línea.

Verificar periódicamente la integridad de los backups y realizar pruebas de recuperación de datos.

Protección de redes:

Configurar firewalls de próxima generación (NGFW) para filtrar el tráfico malicioso.

Segmentar la red de la oficina, aislando dispositivos de alto riesgo (como impresoras) de los servidores principales.

Utilizar una red privada virtual (VPN) segura para conexiones remotas.

Acceso controlado:

Implementar control de acceso basado en roles (RBAC) para limitar el acceso a la información sensible.

Monitorear los accesos y cambios a los expedientes mediante herramientas de auditoría de seguridad.

Capacitación en ciberseguridad:

Realizar capacitaciones periódicas para todos los empleados sobre phishing, ciberseguridad y buenas prácticas en el manejo de datos.

Los abogados están obligados a proteger no solo los documentos físicos, sino también los archivos digitales. Esto incluye el uso de herramientas de encriptación para asegurar el contenido de correos electrónicos y sistemas de almacenamiento en la nube.

Medidas técnicas recomendadas: Utilización de cifrado AES-256 para datos en reposo y en tránsito. Para los correos electrónicos, se debe utilizar PGP o S/MIME (Secure/Multipurpose Internet Mail Extensions) para cifrar y firmar digitalmente los mensajes.

Aseguramiento de dispositivos móviles:

Dado que muchos abogados manejan información confidencial en dispositivos móviles (smartphones, tablets), estos deben estar protegidos por encriptación completa del disco y software de seguridad móvil que prevenga la instalación de apps maliciosas.

V.- Casos prácticos: Lecciones aprendidas de la falta de ciberseguridad.

Caso 1: Ataque de ransomware a un bufete de abogados en Brasil

En 2019, un prestigioso bufete brasileño fue víctima de un ataque de ransomware que comprometió cientos de expedientes confidenciales. Los abogados no tenían una política de

backups adecuada y se vieron obligados a pagar un rescate significativo en criptomonedas para recuperar sus datos. Como resultado, el bufete perdió varios clientes importantes y su reputación se vio gravemente afectada.

Lección: Es imprescindible contar con backups frecuentes, encriptados y almacenados fuera de línea para mitigar el impacto de un ataque de ransomware.

Caso 2: Filtración de correos electrónicos en un estudio en Argentina

Un estudio jurídico mediano en Argentina sufrió la filtración de miles de correos electrónicos debido a una falla en la configuración de su servidor de correo. Los correos contenían información sensible sobre casos en curso, lo que puso en riesgo la defensa de varios clientes y generó posibles acciones legales por negligencia profesional.

Lección: La correcta configuración y protección de los sistemas de correo electrónico, mediante el uso de encriptación y autenticación multifactor, es fundamental para mantener la confidencialidad de la comunicación con los clientes.

Caso 3: Brecha de datos en una firma multinacional

En 2020, una firma multinacional de abogados fue atacada mediante una vulnerabilidad en su plataforma de gestión documental, lo que resultó en la exposición de documentos confidenciales de varias empresas. La brecha fue utilizada por competidores para obtener ventaja en negociaciones de contratos clave.

Lección: La actualización constante de los sistemas de gestión documental y la realización de pruebas de vulnerabilidad son esenciales para prevenir brechas de datos.

VI.- Herramientas gratuitas y de bajo costo recomendadas

Para los estudios jurídicos con presupuestos limitados, existen herramientas de ciberseguridad gratuitas o de bajo costo que pueden ser implementadas fácilmente:

Gestión de contraseñas:

Bitwarden: Un gestor de contraseñas de código abierto que permite almacenar contraseñas de manera segura y ofrece autenticación multifactor.

LastPass (versión gratuita): Permite la gestión básica de contraseñas y el acceso en dispositivos múltiples.

Protección de dispositivos:

Malwarebytes (versión gratuita): Un software antimalware eficaz que escanea y elimina amenazas en tiempo real.

Avast Free Antivirus: Proporciona protección antivirus gratuita con actualizaciones automáticas y protección en la web.

Copias de seguridad:

Duplicati: Software gratuito de código abierto para realizar copias de seguridad encriptadas en la nube o en servidores locales.

Google Drive (versión gratuita): Ofrece almacenamiento gratuito en la nube de hasta 15 GB, útil para copias de seguridad básicas de documentos.

Seguridad de red:

OpenVPN: Solución de código abierto que permite la creación de una red privada virtual (VPN) segura y económica.

pfSense: Un firewall de código abierto que puede instalarse en cualquier hardware compatible para proteger la red de un estudio jurídico.

Monitoreo de seguridad:

Security Onion: Distribución gratuita de Linux diseñada para monitorear redes y detectar intrusos.

Wazuh: Solución gratuita de código abierto que proporciona monitorización de seguridad, detección de intrusiones y análisis de vulnerabilidades.

Capacitación y concientización:

Phishing Box: Herramienta de bajo costo para simular ataques de phishing y capacitar a los empleados en la detección de correos electrónicos fraudulentos.

Cybrary: Plataforma gratuita que ofrece cursos en ciberseguridad, desde lo básico hasta certificaciones avanzadas.

Recomendaciones para fortalecer la ciberseguridad en el ejercicio profesional

Incorporación de prácticas de ciberseguridad en el Código de Ética Profesional

Propuesta para que los colegios de abogados actualicen sus códigos de ética, estableciendo explícitamente la obligación de implementar medidas de ciberseguridad.

Promoción de la formación continua en ciberseguridad:

Los abogados deben participar en capacitaciones periódicas que les permitan conocer las últimas amenazas y las tecnologías emergentes de protección.

VII.- Consideraciones Finales

La ciberseguridad ha dejado de ser un ámbito exclusivo de expertos en tecnología para convertirse en un pilar fundamental del ejercicio profesional de los abogados. La creciente digitalización de los procesos judiciales y la comunicación electrónica impone nuevas responsabilidades éticas, especialmente en la protección de la confidencialidad de la información y los datos personales de los clientes. En este contexto, la falta de adopción de medidas de seguridad adecuadas no solo compromete la reputación profesional, sino que también conlleva riesgos legales que pueden derivar en sanciones civiles y penales.

La actualización de los códigos de ética profesional debe ser vista como una necesidad imperiosa, imponiendo la obligación de implementar protocolos de ciberseguridad que garanticen la integridad de los expedientes digitales. Además, la formación continua en esta materia es esencial para que los abogados puedan anticiparse a las amenazas tecnológicas emergentes y aplicar las mejores prácticas en el manejo de la información sensible.

En conclusión, el abogado moderno debe adoptar una postura proactiva frente a los desafíos de la era digital, integrando la ciberseguridad como una parte central de su responsabilidad ética y profesional. Solo así será posible garantizar la confianza de los clientes y la salvaguarda de los derechos que se les encomiendan, consolidando la abogacía como una profesión comprometida tanto con la justicia como con la seguridad en el entorno digital.

PROPUESTAS

Propuesta 1:

Se propone la inclusión obligatoria de políticas de ciberseguridad en los estudios jurídicos, que incluyan el uso de cifrado en comunicaciones electrónicas y la gestión segura de documentos, con el fin de proteger la confidencialidad de los expedientes digitales y evitar fugas de información.

Propuesta 2:

Se propone que los colegios de abogados exijan a sus matriculados la implementación de autenticación multifactor (MFA) en todas las plataformas utilizadas para la gestión de expedientes digitales y la comunicación con clientes, como medida básica de protección contra accesos no autorizados.

Propuesta 3:

Se sugiere la creación de un protocolo estandarizado de respuesta ante incidentes de seguridad informática en estudios jurídicos, que permita actuar rápidamente ante ciberataques o brechas de seguridad, mitigando daños y preservando la integridad de la información confidencial.

Propuesta 4:

Se propone la creación de un repositorio de herramientas y software de ciberseguridad, gestionado por los colegios de abogados, que incluya recomendaciones de aplicaciones gratuitas o de bajo costo para la gestión segura de contraseñas, cifrado de archivos y comunicaciones.

Propuesta 5:

Se propone incorporar en las capacitaciones obligatorias de los colegios de abogados un módulo específico sobre ciberseguridad aplicada a la abogacía, con el objetivo de mantener a los profesionales actualizados frente a las amenazas cibernéticas emergentes y garantizar la protección de la información sensible.

