GUÍA ICAM

CIBERSEGURIDAD

PARA LA ABOGACÍA

ILUSTRE COLEGIO
DE LA ABOGACÍA
DE MADRID

INTRODUCCIÓN

En el ejercicio de la abogacía, los despachos y profesionales del Derecho manejan información de alta sensibilidad: datos personales, estrategias legales, **documentos confidenciales** y, en muchos casos, secretos empresariales. Este tipo de información es un objetivo atractivo para los ciberdelincuentes, quienes emplean cada vez métodos más sofisticados para acceder a datos valiosos.

Ciberataques como **el phishing, el ransomware, el robo de datos o incluso el espionaje digital** son riesgos reales que pueden comprometer no solo la confidencialidad de la información, sino también la reputación de los despachos y la confianza de sus clientes. Una brecha de seguridad puede resultar en pérdidas económicas, sanciones legales y daños irreparables a la relación abogado-cliente.

Además, el marco normativo, como el **Reglamento General de Protección de Datos (RGPD) en Europa**, exige a los abogados y despachos garantizar un manejo seguro de los datos. El incumplimiento de estas normativas puede derivar en multas significativas, por lo que la ciberseguridad no es solo una buena práctica, sino una obligación legal.

Esta guía del ICAM tiene como objetivo ***brindar a los abogados y despachos de todos los tamaños las herramientas y estrategias necesarias para proteger su entorno digital.***

Desde medidas básicas, como el uso de contraseñas robustas, hasta la implementación de soluciones avanzadas, esta guía pretende ser un recurso práctico para reducir riesgos, proteger la información confidencial y garantizar un nivel de seguridad adecuado en todas las operaciones legales, **ya sea en la oficina o en trabajo remoto.**

EUGENIO RIBÓN
Decano del ICAM

MABEL KLIMT
Diputada del ICAM responsable de innovación y tecnología

ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

AMENAZAS Y CONSECUENCIAS

- **Consecuencias:** Un ciberataque puede tener consecuencias muy graves: **1.Pérdidas de información.** 2. **Pérdidas económicas.** 3. **Crisis de reputación y de confianza.** 4. **Responsabilidad jurídica.** Identifica, en tu caso concreto, qué impacto podría llegar a tener un ataque informático para prevenir sus daños.

- **Amenazas:** Las principales amenazas para la seguridad informática son: 1. **Programas maliciosos** . 2. **Errores en los sistemas, aplicaciones o dispositivos que usamos**. 3. **Los propios usuarios.** 4. **Seguridad física: robos, accidentes, fallos del sistema, fenómenos naturales…** 5. **El propio funcionamiento de un sistema** (por ejemplo, el rastreo permanente de nuestra ubicación en los servicios de telefonía móvil).

- **Tipos de ataques:** **El malware** (programas maliciosos) incluyen virus, troyanos o spyware que dañan o controlan los sistemas. **El ransomware** es un tipo de malware que cifra los archivos, exigiendo un rescate para su liberación. Otros ataques pueden ser de **'denegación de servicio'** haciendo una web o servicio digital inaccesible, desfiguración de webs (cambios en la apariencia o contenidos de una web) o **ataques de ingeniería social.**

- **RECUERDA:** Minimiza todo lo posible los efectos que te puede causar un ciberataque, **en particular creando back-ups** (copias de seguridad) de la información que sea vital. Recuerda que la seguridad total no existe.

ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

¿DÓNDE ESTÁ EL PELIGRO? MAPA DE PUNTOS CRÍTICOS

1 Metadatos

- Lo dicen todo de nuestras comunicaciones: desde dónde nos conectamos, con quién nos comunicamos, qué dispositivos usamos, a qué hora, qué programa y versión usamos, el idioma...

2 Dispositivos

- Robo
- Acceso (físico) por terceras personas
- Virus o conexión de unidades externas no seguras o infectadas (USB, CDs)
- Vulnerabilidades o fallos de hardware o software.
- Control remoto no autorizado

3 Wifi/redes

- Cuando nuestro dispositivo está en redes no seguras se puede acceder al mismo para espiar su contenido

4 Apps Programas

- Vulnerabilidades o brechas
- Rastro de metadatos

5 Actividad y presencia digital

- Navegación
- Intercambio de archivos
- Almacenamiento
- No borrado seguro
- Suplantación de identidad

6 Servicios que usas

- Red, servidores, juegos online, banca o comercio electrónico...Pueden sufrir un ciberataque y poner en riesgo también tus datos.

ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

¿QUÉ ES UNA BRECHA DE SEGURIDAD?

Una brecha de datos personales es un incidente de seguridad que afecta la confidencialidad, integridad o disponibilidad de datos personales, ya sea por acceso no autorizado, pérdida, alteración o divulgación indebida.

En el ámbito de la abogacía y los despachos, estas brechas adquieren especial relevancia debido a la naturaleza confidencial de la información gestionada, lo que hace imprescindible una respuesta adecuada y responsable.

• ¿QUÉ HACER ANTE UNA BRECHA?

Los despachos están obligados a notificar a la Agencia Española de Protección de Datos (AEPD) cualquier brecha que suponga un riesgo para los derechos y libertades de las personas afectadas.

Esta notificación debe realizarse electrónicamente, mediante el formulario disponible en la Sede Electrónica de la AEPD, y en un plazo máximo de 72 horas desde la detección de la brecha.

Cumplir con esta obligación no solo evita posibles sanciones, sino que también demuestra la diligencia y responsabilidad proactiva de la organización.

En los casos en que no exista riesgo, el despacho debe documentar de forma exhaustiva el incidente, describiendo los hechos, sus consecuencias y las medidas adoptadas.

Este registro es fundamental para garantizar la transparencia y permitir a la autoridad de control verificar el cumplimiento normativo.

¿QUÉ CONSECUENCIAS TIENE?

Pérdida de información: La confidencialidad de los casos podría verse comprometida.

Pérdidas económicas: Los ataques pueden paralizar operaciones o implicar gastos en recuperación.

Crisis de reputación y confianza: Un fallo en la seguridad podría afectar la credibilidad del bufete.

Responsabilidad jurídica: Exposición a demandas por negligencia en la protección de datos.

ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

EL PHISHING

Es una variedad de programas espías que se propaga a través del correo con el objetivo de obtener datos confidenciales del usuario. Los correos de phishing están diseñados para tener el mismo aspecto que los que el usuario esperaría recibir de instituciones o marcas conocidas.

Los correos contienen un enlace que redirecciona al usuario a una página falsa que solicita que se introduzcan datos confidenciales.

Esta tendencia se extiende a los sms, llamado smsishing, y a las llamadas telefónicas, llamada vishing.

ASÍ TE ENGAÑAN

- Usar sites similares a direcciones web conocidas para confundirte. Fíjate: http://wwwcnn.com/ es diferente de http://www.cnn.com/
- Otra forma es usar acortadores de URL para camuflar destinos maliciosos. Hay herramientas como https://www.checkshorturl.com/ que permiten ver a dónde nos va a redireccionar el link.
- Los logos corporativos conocidos es otra forma de engaño: que aparezca en un correo no quiere decir que este sea genuino pues son imágenes fáciles de copiar.
- Tampoco debemos fiarnos si el remitente nos resulta conocido en un correo que se nos reenvía como aparentemente devuelto, pues se ha podido cortar ese dato de uno verdadero.

CÓMO EVITAR CAER

- No pinchar enlaces o descargar archivos de correos que temamos estén utilizando estas técnicas.
- Verificar los correos con los remitentes.
- Abrir documentos sospechosos en herramientas en línea para visualizarlos antes de descargar en nuestro equipo.
- Usar métodos de autenticación de correos

ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

BUENAS PRÁCTICAS

CONTRASEÑAS SEGURAS

Crear contraseñas complejas **(mínimo 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos)** para prevenir accesos no autorizados.

Los gestores de contraseñas permiten crear y almacenar contraseñas seguras sin tener que recordarlas todas.

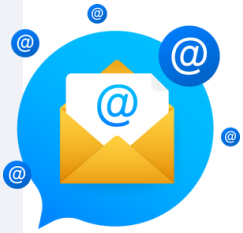
Además, **activar el doble factor de autenticación (2FA)** proporciona una capa adicional de seguridad al requerir un segundo método de verificación, como un código enviado al teléfono móvil.

ACTUALIZACIONES PERIÓDICAS:

Mantener **actualizados los sistemas operativos**, aplicaciones y antivirus garantiza que se instalen parches de seguridad importantes para corregir vulnerabilidades que los atacantes pueden explotar.

EVITAR REDES WI-FI PÚBLICAS

Las redes Wi-Fi públicas **no son seguras**, lo que facilita los ataques. Si es necesario usarlas, se debe usar una VPN (Red Privada Virtual), que cifra la conexión a Internet y protege la información transmitida.



CUIDADO CON LOS CORREOS

No abrir **enlaces ni descargar archivos de remitentes desconocidos.**

Los correos de phishing a menudo incluyen enlaces falsos que dirigen a páginas fraudulentas diseñadas para robar contraseñas. Implementar soluciones antiphishing ayuda a identificar y bloquear estos intentos.

• BUENAS PRÁCTICAS ADICIONALES

Segmentación de redes: Organizar y proteger las conexiones entre los dispositivos de una red dividiéndola en partes más pequeñas llamadas "segmentos".

Copias de seguridad regulares: Hacer copias de seguridad frecuentes de todos los datos importantes y almacenarlas de forma segura, idealmente en un sistema en la nube o en un servidor externo.

Control de acceso: Implementar políticas basadas en roles, asignando permisos según las responsabilidades de cada usuario. Esto asegura que solo el personal autorizado pueda acceder a la información confidencial.

Cifrado de comunicaciones: Utilizar cifrado de extremo a extremo en todas las comunicaciones electrónicas, incluidas las videoconferencias y los correos electrónicos.

Auditorías de seguridad periódicas: Realizar evaluaciones regulares de seguridad para identificar vulnerabilidades en los sistemas y aplicar las correcciones necesarias.

Educación continua: Realizar talleres y simulaciones periódicas sobre ciberseguridad para mantener al equipo actualizado sobre las amenazas y cómo prevenirlas.

ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

¿CÓMO PROTEGER LOS DATOS?

Selecciona proveedores de almacenamiento en la nube que ofrezcan cifrado de datos y cumplan con las normativas de seguridad.

Implementa **controles de acceso** basados en roles para asegurar que solo personal autorizado tenga acceso a información confidencial.

Asegúrate de que los servidores donde se almacenan los datos estén **protegidos con firewalls** y medidas adicionales de seguridad.

Establece procedimientos claros **para eliminar datos** que ya no sean necesarios, como archivos obsoletos o datos de clientes.

Utiliza herramientas de **borrado seguro** para asegurarte de que los datos eliminados no puedan ser recuperados.

Realiza un **auditoría periódica** de los archivos almacenados para identificar información obsoleta que deba ser destruida.

ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

HERRAMIENTAS DE CIBERSEGURIDAD

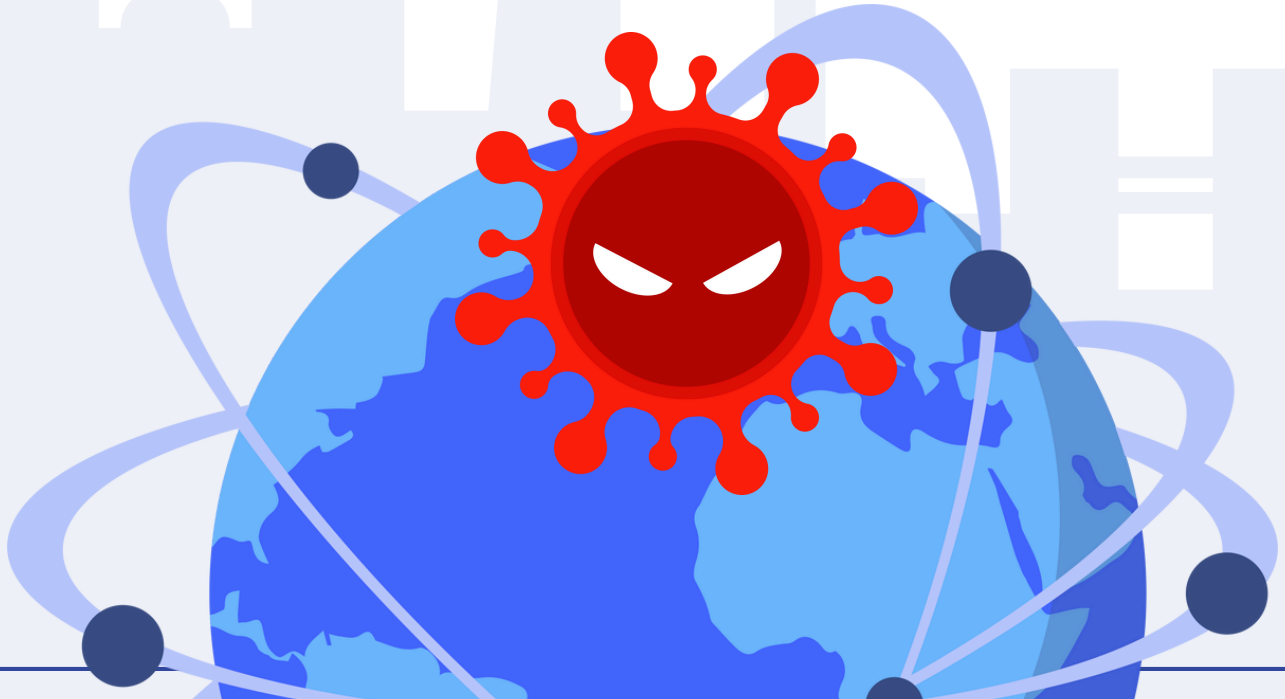
Contar con herramientas tecnológicas adecuadas es crucial para proteger tanto la información confidencial de los clientes como la infraestructura digital del despacho. Estas son algunas de las herramientas esenciales:

- **Antivirus y antimalware:** Los antivirus y programas antimalware protegen los dispositivos contra software malicioso, como virus, spyware, troyanos, y ransomware. Estos programas detectan y eliminan amenazas antes de que puedan afectar el sistema o robar datos.

- VPN (Red Privada Virtual): Una VPN es vital, especialmente cuando los empleados trabajan de forma remota. Cifra la conexión a Internet, asegurando que la transmisión de datos, tanto desde dispositivos personales como corporativos, sea segura y no pueda ser interceptada por terceros. Esto es crucial cuando se usan redes Wi-Fi públicas o conexiones no seguras.

- **Cifrado de datos:** El cifrado protege los datos almacenados en los servidores y durante la transmisión a través de redes, asegurando que solo los usuarios autorizados puedan acceder a la información. En el ámbito legal, es especialmente importante cifrar la información sensible de los clientes, ya que evita que los datos sean expuestos en caso de un ataque cibernético.

- Gestión de dispositivos: Implementar una política de gestión de dispositivos ayuda a controlar qué dispositivos pueden acceder a los sistemas internos del despacho. Esto incluye tanto dispositivos de trabajo como personales (BYOD). Utilizar herramientas de gestión de dispositivos móviles (MDM) permite aplicar políticas de seguridad, como la encriptación de dispositivos, bloqueo remoto y borrado de datos en caso de pérdida o robo del dispositivo.



EL TELETRABAJO

Para garantizar la seguridad en el teletrabajo, es fundamental **evitar que los empleados utilicen sus dispositivos personales** para acceder a los sistemas del despacho, ya que no se puede controlar su nivel de seguridad.

Los equipos personales pueden **carecer de actualizaciones**, antivirus adecuados o configuraciones de protección.

Se recomienda que utilicen equipos proporcionados por el despacho, configurados conforme a las políticas de seguridad. Si se emplean equipos personales, deben contar con medidas estrictas como antivirus, actualizaciones regulares y cifrado.

Adicionalmente, es necesario implementar VPN para cifrar las comunicaciones remotas, especialmente en redes Wi-Fi públicas, y ofrecer educación continua sobre ciberseguridad para reducir riesgos.

FORMACIÓN Y EDUCACIÓN

La educación continua es crucial para garantizar que todos los empleados del despacho estén preparados para identificar y responder a las amenazas cibernéticas.

Capacitación

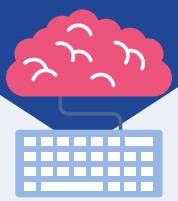
Todos los miembros del equipo deben recibir formación en temas de ciberseguridad, desde la identificación de correos electrónicos sospechosos hasta el manejo seguro de contraseñas y dispositivos.

Simulacros y protocolos

Realizar simulacros de ciberataques para familiarizar a los empleados con los procedimientos de respuesta en caso de brechas de seguridad. Estos simulacros deben incluir cómo identificar incidentes, a quién notificar y cómo mitigar el daño.

Concienciar

Mantener al personal informado sobre las últimas tendencias de ciberamenazas, como phishing o ransomware, para que puedan reconocer estos riesgos de manera temprana y actuar de forma adecuada.



ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

TEST DE CIBERSEGURIDAD

LOS 5 PASOS QUE NO DEBES OLVIDAR PARA ESTAR MÁS PROTEGIDO/A

HAZ UN ANÁLISIS DE RIESGOS Y DE TUS PUNTOS CRÍTICOS.

Valora también el nivel de seguridad que necesitas.

Para ello, algunas preguntas básicas que debes responder son: a) **Qué es lo que necesitas proteger** (por ejemplo: el contenido de tus comunicaciones, tu identidad, los metadatos, todo ello...), b) **de quién te quieres proteger** y cuál es su capacidad de ataque c) qué probabilidad hay de que sufras los distintos tipos de ataque, d) cómo de graves son las consecuencias, e) **cómo es de costoso** o problemático la prevención del ataque.

LA SEGURIDAD TOTAL NO EXISTE.

Ante esto, lo mejor **es minimizar las amenazas** y su capacidad para afectarte: Mantén actualizados tus equipos y antivirus, guarda copias de seguridad de tus documentos y, si puedes, usa siempre software libre.

En ocasiones te puede interesar **tener dispositivos distintos de los que uses normalmente** sólo para usos específicos (viajes a destinos donde te los puedan inspeccionar o robar, contacto con fuentes sensibles), e incluso equipos que nunca hayas conectado a Internet para mejorar aún más la seguridad ("airgapped")

NUNCA OLVIDES QUE EL FACTOR HUMANO (TÚ) ES EL ESLABÓN MÁS DÉBIL EN LA SEGURIDAD.

Ten cuidado con los **archivos que descargas, los enlaces que pinchas, los dispositivos que se conectan a tus equipos** o las redes a las que te conectas. Estate prevenido frente a ataques por "phising" y otras técnicas de ingeniería social.

USA HERRAMIENTAS DE CIFRADO PARA MANTENER LA PRIVACIDAD DE TUS COMUNICACIONES SI ES NECESARIO

Clientes de correo electrónico y aplicaciones de chat o videollamada con cifrado de extremo a extremo

ELIGE CONTRASEÑAS FUERTES, DISTINTAS PARA CADA DISPOSITIVO Y CÁMBIALAS PERIÓDICAMENTE.

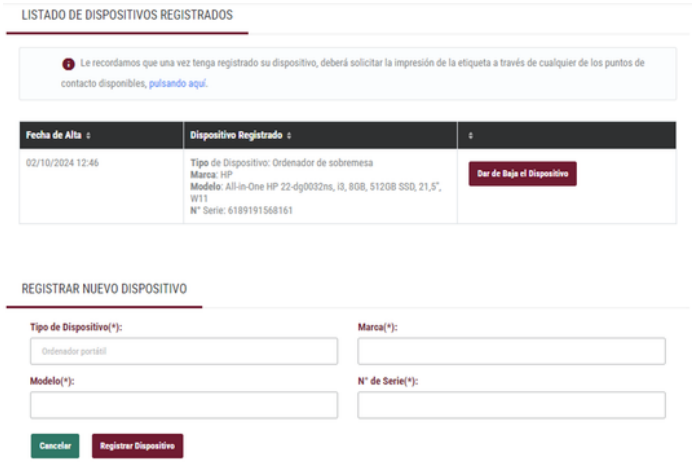
ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID

AMPARO DE DISPOSITIVOS ICAM

El servicio Amparo de Dispositivos se implementa como una solución integral para la gestión de dispositivos tecnológicos de los profesionales ejercientes del ICAM. Además de facilitar un control eficiente y seguro de estos equipos, el servicio incluye un sello para etiquetar dispositivos, buscando reforzar la protección de los activos tecnológicos y la información confidencial que contienen.

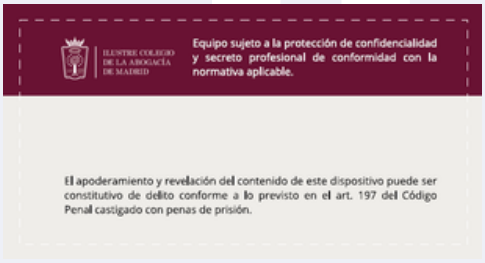
Su funcionalidad principal consiste en p**ermitir a los usuarios registrar hasta un máximo de 10 dispositivos** (ordenadores portátiles, de sobremesa, móviles o tablets) que utilizan en su práctica profesional.

Este servicio estará disponible a través del área reservada de nuestra página web de manera fácil y segura en **“Servicios Colegiales >> Trámites”.**



El proceso de registro es ágil; una vez que se completan estos campos, se muestra una confirmación en pantalla junto con las instrucciones necesarias para imprimir **la etiqueta identificativa correspondiente al dispositivo registrado.**

Esta etiqueta colegial es **específica para las personas profesionales de la abogacía** que trabajen por cuenta propia o en régimen de dependencia laboral para empresas o similares, con el objetivo de acreditar el amparo de sus dispositivos tecnológicos.



GUÍA ICAM

CIBERSEGURIDAD

PARA LA ABOGACÍA

ILUSTRE COLEGIO
DE LA ABOGACÍA
DE MADRID