Módulo 2. Seguridad, autenticación y marco legal argentino

Es variada la legislación que existe en cada país. Si bien hay un hilo conductor que entiende y tipifica el delito informático en el Código Penal, en Argentina se han aprobado leyes específicas de este tema con base en acontecimientos o sucesos que han ocurrido.

El primer módulo nos introduce en el mundo de la ciberseguridad y nos permite apreciar que las vulnerabilidades pueden estar presentes desde el momento mismo de entrada o salida a un edificio y alcanzan hasta lo más complejo de las comunicaciones. Uno de los aspectos importantes de la ciberseguridad que veremos en este módulo es asegurar que los diálogos entre los emisores y receptores sean seguros entre ellos. Esto se logra por medio de la criptografía que encripta la información para que viaje seguro. Hay que tener presente también que, la detección de anomalías en una red se logra mediante el monitoreo constante de la información que transita por la misma, lo que hace que se deba tener especial cuidado de ser vista por potenciales curiosos.

Esto nos recuerda a la característica que debe poseer la información en cuanto a **confidencialidad, integridad y disponibilidad,** que deberán estar presentes en todo momento a pesar de la monitorización que se realice sobre la información en una red, control de acceso y autentificación.

“La necesidad de ocultar información al enviar mensajes tiene su origen en tiempos inmemoriales. La historia refiere muchos eventos de diversas guerras muy antiguas, cuando era necesario enviar mensajes de un ejército en el campo de batalla a las autoridades, gobernantes o reyes de alguno de los países en guerra. Mensajes que, de ser interceptados por el enemigo, hubieran podido inclinar la victoria hacia una de las partes beligerantes, por lo que ya desde entonces se hablaba de mensajes encriptados” (Baca Urbina, 2016, p. 58).

1. Vulnerabilidades

Vulnerabilidades

Cuando hablamos de vulnerabilidades, tenemos que hacer referencia también a las amenazas de seguridad que constituyen una probabilidad de violación. Estas amenazas pueden generar un cambio intencional no autorizado del estado en un sistema o que haya fuga de información como el robo de contraseñas, escalar privilegios, etc. Las **vulnerabilidades** permiten concretar una amenaza y pueden estar presentes desde el minuto cero y son llamadas vulnerabilidades *zero day* (OSI, 2020).

Algunas vulnerabilidades responden a fallas en el diseño, la no previsión de cambios, errores de programación, etc.; y otras pueden ser intencionalmente diseñadas para ciberespionaje, como la obtención de datos financieros de las víctimas o la obtención del tráfico (paquetes) por parte de gobiernos. Eduard Snowden ya había dado a conocer el sistema que funciona bajo el nombre Quantum (Welle, 2013). Es por ello que toman relevancia los conceptos como *zero trust* (confianza cero), un modelo de

seguridad que parte de la premisa de “nunca confiar, siempre verificar”, y elimina la confianza implícita en cualquier usuario o dispositivo, estén dentro o fuera de la red, y exigiendo una autenticación y autorización rigurosa para cada acceso a recursos, protegiendo así contra amenazas internas y externas en entornos modernos de trabajo remoto y nube.

Vector de ataque

Un vector de ataque es un método que utiliza una amenaza para atacar un sistema. Los vectores de ataque en ciberseguridad son las formas o medios que permiten a ciberdelincuentes transmitir códigos maliciosos. La metodología de trabajo suele ser realizada de la siguiente forma:

1. **“Análisis e inspección del objetivo potencial.** Uso de métodos como *sniffing* (olfatear la red por medio de programas que permiten capturar información), correo electrónico, *malware* o ingeniería social.

2. **Codificación.** Se codifican y alinean las herramientas para efectuar el ataque.

3. **Instalación.** Se infiltra la seguridad y se instalan los softwares maliciosos que abrirán las puertas de ataque.

4 **Explotación.** Vulnerados los sistemas; se explota la información (data sensible) para obtener los beneficios pretendidos y comprometer las defensas del atacado" (Alfanumeric, s.f., https://n9.cl/bkwew).

Algunos **vectores de ataque** son:

- Credenciales comprometidas: incluyen estafas de *phishing*, fugas de datos, infecciones de *malware* o simplemente el hábito clásico de usar contraseñas débiles o reutilizar las mismas contraseñas en varias cuentas.

- *Phishing*: esta es una de las formas más tradicionales de ingeniería social, donde los principales objetivos son los humanos y sus actos predecibles al abrir un correo electrónico.

- Vulnerabilidades sin parchear: los ciberdelincuentes utilizan este vector de ataque para entrar en sistemas y *software*. Aprovechar estas vulnerabilidades es algo fácil después de encontrar el CVE (más adelante se describe el significado del mismo) o PoC correcto.

- Cifrado deficiente o faltante: hay personas que utilizan sesiones FTP sin cifrar para transferir datos, o que pasan datos a través de un protocolo HTTP simple sin cifrado TLS.

- Configuración incorrecta: el uso de la configuración predeterminada en los dispositivos de hardware y las aplicaciones de software, exposición pública de datos, o la configuración incorrecta de cualquier configuración, podría hacer que tus servicios sean explotados debido a vulnerabilidades conocidas y desconocidas.

- *Insiders* maliciosos: este vector de ataque involucra a empleados con malas intenciones. Comparten información privada y sensible sobre *software*, servidores o dispositivos relacionados con el hardware con un tercero, quien luego puede usar esta información para causar daños a la empresa.

- *Ransomware*: el método más utilizado es obtener acceso al sistema, bloquear y cifrar los datos del disco duro y luego solicitar el pago para liberar la clave de descifrado.

- Proveedores externos: la subcontratación es una de las mejores formas de obtener ventajas estratégicas, reducir costos y aportar valor técnico y comercial a tu empresa. Sin

embargo, la desventaja de esto es que está dejando a tu organización expuesta a un nuevo riesgo de ciberseguridad. Los proveedores externos también pueden ser la principal causa de pérdida de datos, violaciones de seguridad y fugas de datos.

Investigación sugerida: Los tres vectores de ataque más comunes que explotan los documentos de Office se pueden observar en el siguiente *link:* https://n9.cl/8mv4b.

A pesar de las constantes y distintas medidas de seguridad, los *hackers*, ingeniosa y creativamente, explotan todo tipo de vulnerabilidades, especialmente las de gran impacto donde posiblemente pueden haber sido aprovechadas silenciosamente durante mucho tiempo.

Una gran vulnerabilidad catalogada con el nivel más alto de criticidad y el que ha motivado titulares periodísticos como *Log4Shell, el fallo del siglo que ha puesto a Internet de rodillas* (El Mundo, 2021), data de mediados de diciembre de 2021 y está registrada como CVE-2021-44228 y CVE-2021-45046. Este hecho ha obligado a muchos proveedores de servicios de ciberseguridad, como los antivirus, a revisar sus servidores para resolver o verificar situaciones que le podrían traer problemas en un futuro cercano. Para entender más acerca de esta situación, se recomienda leer: https://n9.cl/kn5ju.

Hacking ético

Ethical hacking es un proceso de detección de vulnerabilidades en una aplicación, sistema o la infraestructura crítica de una organización donde un atacante puede usar *exploit* para explotar esa debilidad. Cabe aclarar que un *exploit* es un código, *software* o

técnica que se aprovecha de una vulnerabilidad (un fallo de seguridad) en un sistema, aplicación o dispositivo para alterar su funcionamiento normal, con el objetivo de obtener acceso no autorizado, ejecutar comandos maliciosos o robar información.

El *hacking* ético se realiza con el fin de prevenir ciberataques o violaciones de seguridad al intentar comprometer el sistema, infraestructura crítica, etc., en busca de puntos débiles. Se realiza en forma controlada con el aval del destinatario y, por lo general, se firman contratos de confidencialidad donde se indicarán los días y horas en que se realizarán las acciones para que la prueba no provoque un daño mayor al de reportar las debilidades.

En líneas generales, el *hacking* ético busca solucionar fallos de seguridad y prevenir la cibercriminalidad (IONOS, 2020).

Se deja un video recomendado:

Daniel DataShow (2 de junio de 2012). *Historia de los Hackers Informáticos. Los inicios* [archivo de video]. YouTube. https://n9.cl/8cbow.

Entender cómo funcionan los *malware*, propagación, formas de contagio, vectores de ataques, etc., permite la toma de decisiones para contrarrestar acciones mediante evidencia científica.

Pentesting

Las personas que realizan *hacking* ético realizan test de penetración (*penetration test*) sobre infraestructuras críticas, sistemas, etc.

El *penetration testing* es una "metodología que consiste en planificar un ataque a una red, independientemente de su tamaño, o sobre equipos individuales, con el fin de revelar vulnerabilidades en el objeto de prueba. Para este propósito se simulan diversos patrones de ataque utilizando herramientas creadas por métodos de ataque conocidos" (IONOS, 2017, https://n9.cl/g54kg5).

"Entre las otras pruebas de rutina realizadas en el *ethical hacking*, se incluyen la detección de puertos abiertos mediante escaneos de puertos, la verificación de la seguridad de los datos de pago (datos de tarjetas de crédito), los inicios de sesión y las contraseñas y la simulación de ataques a través de la red. Dado que para estas pruebas se suele utilizar el protocolo TCP/IP, también se denominan pruebas de penetración basadas en IP. En las pruebas de penetración, los sistemas se comprueban a menudo para ver si los virus o troyanos infiltrados pueden capturar datos sensibles de la empresa (secretos de empresa, patentes técnicas, etc.). Estas estrategias pueden complementarse con técnicas de ingeniería social, que tienen en cuenta el factor humano de riesgo y examinan explícitamente el comportamiento de los empleados en un concepto de seguridad" (Educación IT, s.f., https://n9.cl/nvqom).

Los estándares a los que los profesionales se refieren son exclusivamente internacionales, a saber:

- **PTES (*penetration testing execution standard*):** El estándar de ejecución de pruebas de penetración consta de siete secciones principales.

- **OSSTMM (*open source security testing methodology manual*):** https://n9.cl/7ijed.

- **OWASP:** El Proyecto Web Security Testing Guide (WSTG) https://n9.cl/0ozcc. Este proyecto "produce el principal recurso de prueba de ciberseguridad para desarrolladores de aplicaciones web y profesionales de la seguridad. El WSTG es una guía completa para probar la seguridad de las aplicaciones web y los servicios web. Creado por los esfuerzos colaborativos de los profesionales de la ciberseguridad y los voluntarios dedicados, el WSTG proporciona un marco de mejores prácticas utilizadas por los probadores de penetración y las organizaciones de todo el mundo" (Panelmega, s.f,, https://n9.cl/fst0u).

> “Las grandes empresas como Facebook, Google y Microsoft utilizan **programas de recompensa** por errores, en los que definen con precisión las condiciones y requisitos para los ciberataques y la búsqueda de errores y, a veces, ofrecen a los hackers exitosos la perspectiva de considerables recompensas financieras para detectar problemas de seguridad. Los programas de recompensa por errores son complementados, la mayoría de las veces, por pruebas de penetración” (IONOS, 2020, https://n9.cl/16fs6).

Historia de la criptografía

“La palabra cripta proviene del griego y significa esconder o encubrir. La Real Academia Española (RAE) la define como un lugar subterráneo donde se enterraba a los muertos. Por extensión, la criptografía se define como el arte de escribir con claves secretas o de manera enigmática. Así, la criptología se considera un tratado acerca de los escritos secretos o cifrados, un criptograma es un documento cifrado y el criptoanálisis es el arte de descifrar criptogramas” (Baca Urbina, 2016, p. 58).

La criptografía moderna nace durante la Segunda Guerra Mundial, siendo Alan Turing uno de los científicos más destacados del momento y cuya área sigue en continuo crecimiento. La criptografía es una ciencia que se convierte en la piedra angular del comercio electrónico (por ejemplo,. Gmail ofrece la opción de encriptar correos electrónicos), se emplea en servicios de

mensajerías (Signal, Telegram, WhatsApp), seguridad para conexión inalámbrica en *router*, los decodificadores de las plataformas de distribución de contenidos multimediales como DirecTV y con el especial uso que se le da a los asuntos militares.

Cifrado simétrico

Muchos sistemas de encriptación usaron sistemas de única clave para desencriptar (simétrica), donde "tanto el emisor como el receptor del mensaje tienen una llave o clave secreta que se utiliza ya sea para cifrar o para descifrar el mensaje" (Baca Urbina, 2016, p. 76). Algunos algoritmos que cifran simétricamente son: AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard), ChaCha20, etc.

"Los ataques por fuerza bruta son el enemigo real de los algoritmos de criptografía simétrica; hay que tener en cuenta que estos algoritmos son públicos y que la fuerza de los mismos depende directamente de lo complejo que sea el algoritmo internamente, y también de la longitud de la clave empleada para evitar estos ataques" (López, 2025, https://n9.cl/f4v9p).

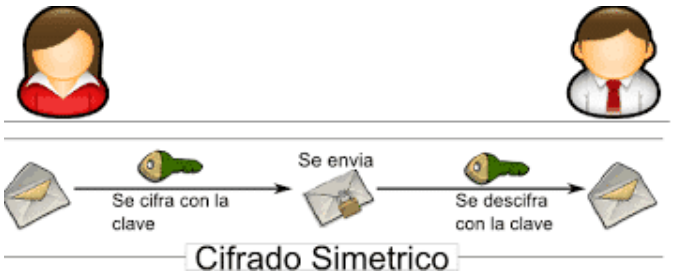
Los algoritmos de criptografía simétrica son de mejor *performance* que los asimétricos. En la actualidad, muchos equipos ya vienen con aceleración de cifrado por *hardware* como en los procesadores (CPU) de Pc, *notebooks*, servidores, *routers*,

etc. Por su velocidad y seguridad los algoritmos más usados son AES y ChaCha20.

Algoritmos simétricos

Este algoritmo se muestra en la siguiente figura.

Figura 1: Algoritmo simétrico



Fuente: [imagen sin título sobre algoritmo simétrico], 2017, https://n9.cl/h872b.

AES

“El algoritmo simétrico AES sustituyó al DES, y es el empleado actualmente en todos los canales y protocolos seguros como TLS, FTPES, redes privadas virtuales (VPN) y mucho más. El cifrado de AES puede ser empleado tanto en *software* como en *hardware*, AES es un algoritmo de cifrado por bloques, y el tamaño fijo del bloque es de 128 bits. La longitud de la clave se puede elegir, y tenemos disponible 128, 192 y 256 bits, siendo la longitud de 128

bits el estándar, pero también son muy utilizados los 256 bits" (López, 2025, https://n9.cl/f4v9p).

Aprovechamos para definir que una VPN (red privada virtual) es un servicio que crea un túnel seguro y cifrado entre tu dispositivo e Internet, enmascarando tu dirección IP y actividad *online* para proteger tu privacidad, seguridad y permitir el acceso a contenido restringido, simulando que te conectas desde otra ubicación.

ChaCha20

"El algoritmo ChaCha20 es un algoritmo de cifrado simétrico que soporta claves de 128 y 256 bits y de alta velocidad; a diferencia de AES, que es un cifrado por bloques, ChaCha20 es un cifrado de flujo" (López, 2025, https://n9.cl/f4v9p).

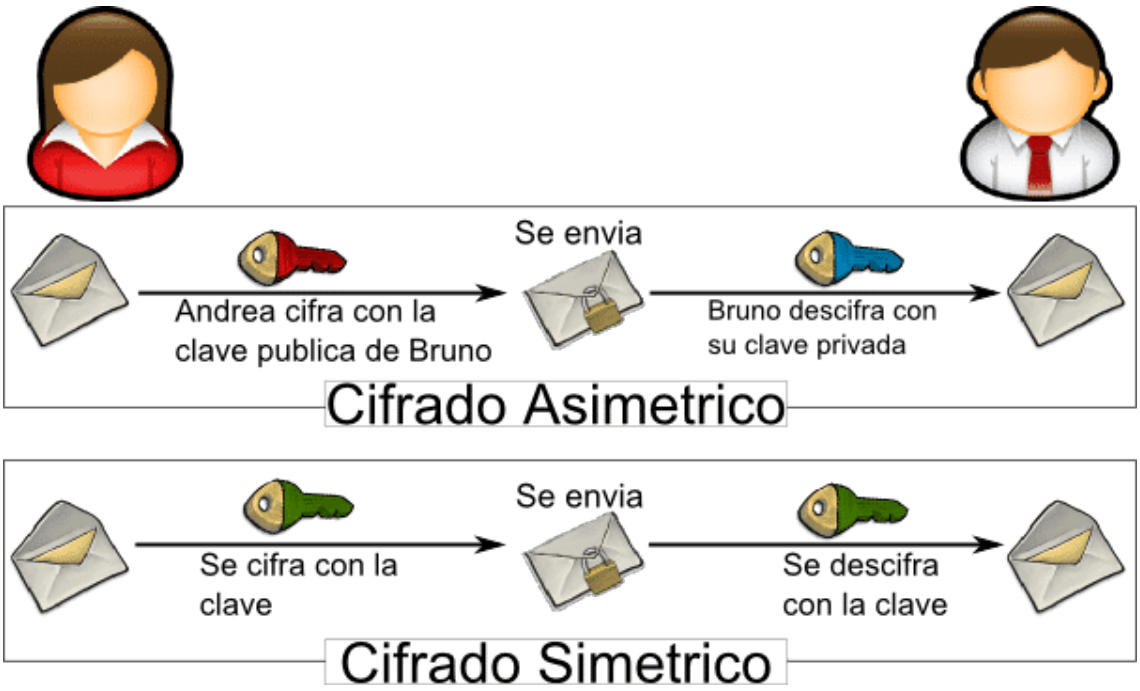
Este algoritmo se utiliza ampliamente en las conexiones HTTPS, en las conexiones SSH para administrar servidores e incluso en el popular protocolo de VPN WireGuard.

Cifrado asimétrico

"Además del cifrado simétrico, también existe el cifrado asimétrico, que requiere de dos claves o llaves: una pública y la otra privada, las cuales están relacionadas matemáticamente" (Baca Urbina, 2016, p. 77). En este esquema de cifrado asimétrico, si un usuario A quiere enviar un mensaje al usuario B, debe utilizar una clave

pública del usuario B para cifrar y enviar el mensaje, cuando el usuario B recibe el mensaje, utiliza su clave privada para descifrarlo (ejemplo de uso WhatsApp, Firma Digital, Telegram, etc.).

Figura 2: Algoritmo asimétrico



Fuente: [imagen sin título sobre algoritmo asimétrico], 2017, https://n9.cl/h872b.

> "La fortaleza del sistema por el cual es seguro este tipo de algoritmo asimétrico es que está basado en funciones matemáticas. Las claves públicas y privadas se generan simultáneamente y están ligadas la una a la otra. La relación entre ambas debe ser muy compleja, para que resulte muy difícil que obtengamos una clave a partir de la otra, en este caso, que obtengamos la clave privada,

puesto que la pública la conoce toda persona conectada al sistema" (López, 2025, https://n9.cl/f4v9p).

Combinación de cifrados asimétrico y simétrico

"El principal inconveniente que tiene este tipo de cifrado es la lentitud; el empleo de este tipo de claves ralentiza el proceso de cifrado de la comunicación.

Esta combinación de cifrados sucede de la siguiente manera. Creamos la clave del algoritmo simétrico, la ciframos con la clave pública del receptor, enviamos los datos cifrados por el canal de comunicación inseguro, y a continuación, el receptor descifrará los datos mediante su llave privada. Con la clave del algoritmo simétrico en los dos puntos, es cuando puede empezar la comunicación mediante el cifrado simétrico, lo que hace que la comunicación sea mucho más rápida que si usáramos solo criptografía asimétrica en toda la comunicación.

Se usa este tipo de método combinado en OpenVPN o IPsec; en ellas, la clave de sesión que es conocida por los usuarios se regenera cada cierto tiempo para incrementar aún más la seguridad en la comunicación, sin que ello conlleve un retardo significativo en la transferencia de los datos" (López, 2025, https://n9.cl/f4v9p).

Desafío-Respuesta

Para aumentar la seguridad, este método comprueba que el emisor es realmente quien dice ser. Para ello, se envía un texto al emisor y este lo cifrará con su clave privada (lo que está haciendo realmente es firmarlo), el emisor nos enviará el texto cifrado (firmado) y nosotros descifraremos la clave (comprobaremos la firma) aprovechando que tenemos la clave pública del emisor, y, por último, compararemos que el mensaje obtenido sea el mismo que enviamos anteriormente.

Si algún usuario se hace pasar por el emisor real, no tendría la clave privada, por lo que el «desafío» no hubiera resultado satisfactorio y no se establecería la comunicación de los datos.

CONTINUAR

2. Firma electrónica o digital y su autentificación

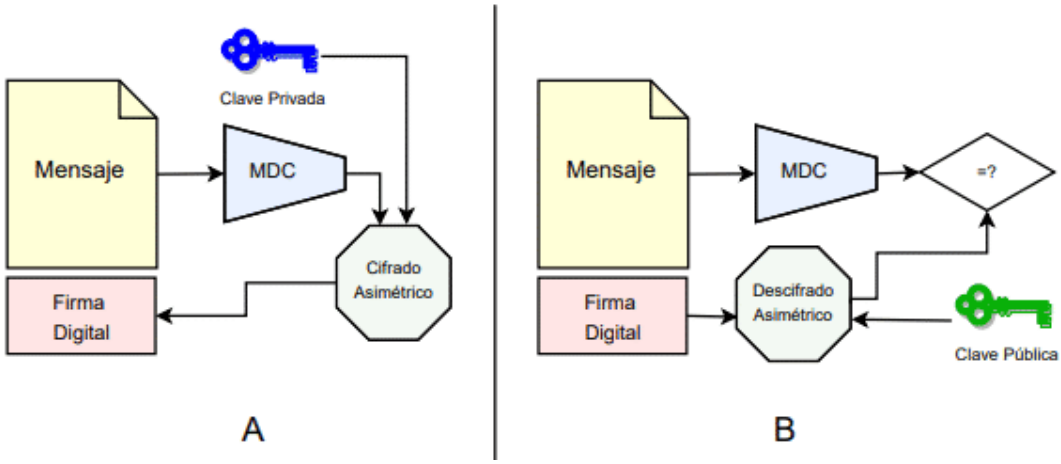
Firma electrónica o digital y su autentificación

Introducción

En el mundo, la firma digital o electrónica es muy utilizada y en cada país recibe un respaldo legal que permite ser implementada según necesidades, por ejemplo, la firma de sentencias judiciales mediante un *token*, la aceptación de pagos mediante dispositivos *posnet*, *lapos*, etc. Durante la pandemia por covid-19, la firma estampada en documentos públicos se utilizó para recibir pagos *online* y autorizar el retiro de dinero.

Philip Zimmenman, en 1991, desarrolló el *software* PGP (*pretty good privacy*, privacidad bastante buena), que se utiliza para el cifrado asimétrico o de clave pública y sirve para enviar información por Internet, mediante el uso de la autenticación de documentos por medio de firmas digitales (Phil Zimmermann & Associates LLC, s.f.).

Figura 3: Esquema de una firma digital basada cifrado asimétricos



Fuente: Lucena López, 2022, p. 304.

Firma digital

Introducción

La firma digital permite al receptor de un mensaje determinar si el origen es auténtico y comprobar si el mensaje ha sido modificado. Una firma digital es una secuencia de bits que se añade a una pieza de información cualquiera, y que permite garantizar su autenticidad de forma independiente del proceso de transmisión, tantas veces como se desee. Presenta una analogía directa con la firma manuscrita (es casi imposible falsificarla), y para que sea equiparable a esta última debe cumplir las siguientes propiedades:

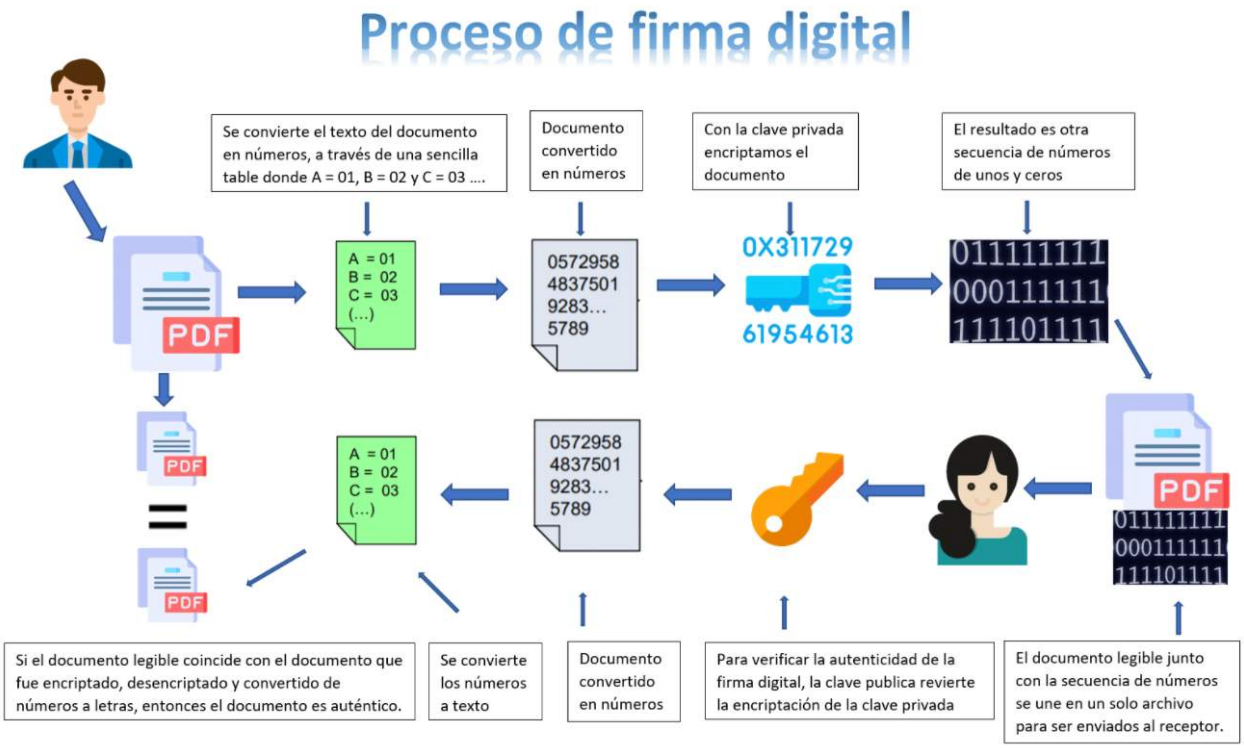
- Una firma digital válida para un documento no puede ser válida para otro distinto.

- Solo puede ser generada por su legítimo titular (por medio de su clave privada). Al igual que cada persona tiene una forma diferente de escribir, y que la escritura de dos personas diferentes puede ser distinguida mediante análisis caligráficos, una firma digital solo puede ser construida por la persona o personas a quienes legalmente corresponde.

- Es públicamente verificable. Cualquiera puede comprobar su autenticidad.

En resumen, la firma digital realiza los siguientes pasos:

Figura 4: Proceso de firma digital



Fuente: elaboración propia.

“En la firma digital se utilizan las funciones hash como SHA2-256 y SHA2-512 donde el emisor de la comunicación aplica la función HASH al mensaje original para obtener con ello la huella digital y luego cifra los datos usando su clave privada y lo envía al receptor por un canal disponible.

Verificar la firma: el receptor descifra los datos usando la clave pública del emisor y comprueba que la información coincide con los datos originales (si coincide es que no se ha modificado).

El destinatario también aplicará la función *hash* a sus datos y comparará los resultados (la que ha obtenido y la que ha recibido).

Si en el resultado de la comparación de estos datos hay diferencias entre lo obtenido y lo recibido, quiere decir que la información ha sido alterada y los datos de la huella digital habrán cambiado. Si el resultado es el mismo, se llevará a cabo la comunicación sin problemas" (López, 2025, https://n9.cl/f4v9p).

Este proceso que se realiza permite saber:

"Autenticidad, el emisor es quien dice ser. La firma en origen y destino es la misma.

Integridad, el mensaje no ha sido modificado. Lo obtenido y lo recibido es igual.

No repudio, el emisor no puede negar haber enviado el mensaje al receptor. La firma digital no varía.

Si queremos introducir la ***confidencialidad*** a la comunicación, lo único que hay que hacer es que el emisor cifre el mensaje original con la clave pública del receptor.

En Argentina, la firma digital tiene:

- **Validez jurídica:** Los documentos electrónicos firmados digitalmente tienen la misma validez jurídica que aquellos firmados de forma hológrafa.

- **Autenticidad e integridad:** Se puede identificar al autor fácilmente y verificar si ese documento fue alterado.

- **Seguridad:** Garantizada por la criptografía asimétrica. Contamos con el respaldo de instalaciones seguras y confiables para el almacenamiento de datos biométricos.

- **Múltiples usos:** Se puede realizar trámites con entidades públicas y privadas firmando cualquier tipo de archivos" (López, 2025, https://n9.cl/f4v9p).

Algoritmos asimétricos

Diffie-Hellman

"Se emplea para obtener la clave privada con la que posteriormente se cifrará la información junto con un algoritmo de cifrado simétrico. Puede sufrir el ataque *man-in-the middle,* ya que si un tercero interfiere en la comunicación, al no poder validar la identidad de usuarios, ya que no proporciona autentificación, le facilitaría las claves y, por lo tanto, podría establecer comunicación entre el emisor y receptor suplantando identidades. Para evitar esto existen varias soluciones que mitigan y solucionan el problema, como hacer uso de certificados digitales" (López, 2025, https://n9.cl/f4v9p).

RSA

Este algoritmo es seguro y utiliza una longitud de 2048 bits, aunque es recomendable que sea de 4096 bits o superior. Se basa en la pareja de claves, la pública y la privada. Es eficiente en el uso de firmas digitales y, en la actualidad, casi el único cuidado a tener en cuenta es que la clave privada debe ser cifrada por algún algoritmo simétrico.

DSA

“Este algoritmo se utiliza ampliamente en las conexiones SSH para comprobar la firma digital de los clientes. Está disponible en todas las librerías criptográficas actuales como OpenSSL, GnuTLS o LibreSSL. Su longitud de clave mínima es de 512 bits, aunque lo más habitual es usar 1024 bits” (López, 2025, https://n9.cl/f4v9p).

Certificado

El Registro Civil de la República Argentina emite la partida de nacimiento de los niños y niñas nacidos en el territorio nacional. Este documento constituye la base de su identidad legal, ya que habilita no solo el reconocimiento de la ciudadanía, sino también la posterior emisión del Documento Nacional de Identidad (DNI) y del pasaporte. Cada vez que sea necesario acreditar la identidad de una persona, los documentos emitidos permiten corroborar sus datos en el Registro Nacional de las Personas (RENAPER), que

actúa como entidad madre y garante de la validación oficial de la identidad.

De igual manera sucede cuando un certificado digital es emitido por una autoridad de certificación. “Un certificado es una confirmación de identidad y contiene información que se utiliza para proteger datos, establecer conexiones seguras de red, proteger al *software* de alteraciones después de su publicación, etc. De este modo, el almacén de certificados, como su nombre lo indica, es el área del sistema donde se guardan los certificados” (Baca Urbina, 2016, p. 109).

Todos los certificados deben cumplir con estándares de seguridad provistos por normas internacionales que avalan la misma, tales como la ISO / IEC 9594-8, cuyo formato general contiene datos como: versión, número de serie, algoritmo de firma, período de validez, propietario del certificado, atributos, identidad del emisor, algoritmo de clave pública, firma de emisor.

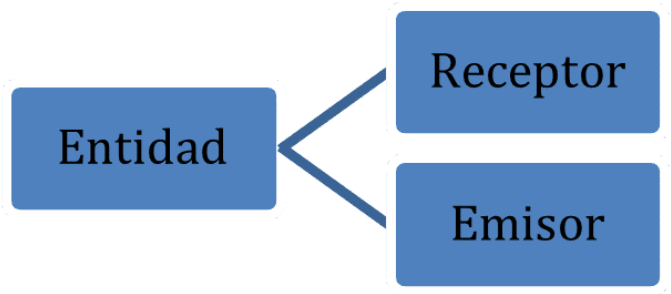
> “Con los datos que muestra un certificado, la infraestructura de clave pública (***public key infrastructure*** o PKI), verifica que el usuario es quien dice ser, ya que el usuario posee un certificado de atributos emitido por una autoridad de atributos, cuyas funciones y concepto pertenecen a una infraestructura de administración de privilegios (PMI, por sus siglas en inglés)” (Baca Urbina, 2016, p. 111).

Puedes leer más acerca de qué es una PKI en el siguiente enlace: https://tinyurl.com/what-is-pki-entrust.

Certificado digital

Es conocido también como certificado electrónico o certificado de clave pública; es un archivo creado por una organización pública o privada (entidad certificante), que ofrece servicios de certificación y crea datos de identidad de una persona física o empresa, dándole una identidad digital en Internet.

Figura 5: Certificado digital



Fuente: elaboración propia.

"Un certificado digital se utiliza para varias cosas, la principal, sin duda, es autenticar la identidad de las partes que intervienen en el intercambio de información: el emisor y el receptor. Cuando se hace intercambio de información, en general se necesita una firma

electrónica, que es la que garantiza tanto la integridad de los datos, como su confidencialidad y el sitio de su procedencia. Garantizar la integridad de los datos implica que estos no sean alterados en su viaje por las redes. La confidencialidad implica que solo las partes interesadas pueden conocer su contenido y nadie más" (Baca Urbina, 2016, p. 112).

Certificados de revocación

Cuando una clave pública pierde su validez (por ejemplo, por destrucción o robo de la clave privada correspondiente), es necesario anularla. Para ello se emplean los denominados certificados de revocación, que no son más que un mensaje que identifica a la clave pública que se desea anular, firmada por la clave privada correspondiente. De esta forma se garantiza que una clave pública únicamente puede ser revocada por su legítimo propietario (si la clave privada resulta comprometida, al atacante no le interesara revocarla, ya que entonces el material robado perdería su valor). Como podemos observar, para revocar una clave pública es necesario estar en posesión de la privada, por lo que, si perdemos esta última, jamás podremos hacer la revocación.

Para evitar estos problemas, conviene seguir una serie de pautas:

- Generar los pares de claves con un período limitado de validez. De esta forma, si no

podemos revocar una clave, expirará por sí misma.

- Generar el certificado de revocación junto con el propio par de claves, y almacenarlo en lugar seguro.

- Algunos protocolos permiten nombrar revocadores para nuestra clave pública, que podrán generar un certificado de revocación empleando únicamente sus propias claves privadas.

Si una clave ha sido anulada por alguna causa, las autoridades que la hubieran certificado deben cancelar todos sus certificados asociados. Esto hace que todas las autoridades dispongan de listas de revocación de certificados (CRL), que se actualizan periódicamente, además de un servicio de consulta de las mismas. Dicho servicio suele permitir tanto la consulta de la validez de un certificado concreto, como la descarga total o parcial de la CRL correspondiente.

Verificación de certificados digitales

Una autoridad de certificación suele tener un ámbito relativamente local, como puede ser una empresa, un campus universitario o un país entero. Si fuera necesario verificar un certificado digital de un certificador ajeno, del cual desconocemos

su fiabilidad, existe la posibilidad de que la clave pública del propio certificador esté a su vez firmada por otra entidad de la que sí nos fiemos, y de esta forma propagar nuestra confianza hacia la entidad certificadora en cuestión. Esta circunstancia puede ser aprovechada de forma jerárquica —como en las PKI (infraestructuras de clave pública o, en inglés, *public key infrastructure*)— o distribuida —como hace PGP.

Firma electrónica

Figura 6: Firma electrónica

Fuente: Iprofesional, 2020, https://n9.cl/6wk98t.

“No es lo mismo una firma electrónica que una digital, y su validez también cambia por países.

. . .

Tanto la **firma electrónica como la digital**, **tienen validez jurídica**, pero la firma electrónica no reemplaza a la manuscrita, ya que no cumple con las propiedades necesarias como si lo hace la firma digital, además del valor probatorio que tiene esta última.

La validez probatoria de la firma digital la hace superior a la electrónica, garantizando la legalidad y transparencia de los documentos firmados digitalmente como prueba legal.

. . .

La Autoridad de Aplicación del régimen normativo que establece la infraestructura de firma digital estipulada por la Ley nro. 25.506 es la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros.

. . .

La firma electrónica es un conjunto de datos electrónicos que acompañan a una determinada información, también en formato electrónico.

Realizar una firma electrónica quiere decir que una persona física verifica una acción o procedimiento mediante un medio electrónico, dejando un registro de la fecha y hora de la misma.

Existen diferentes tipos de firmas electrónicas, cada una con su propio conjunto de requisitos y métodos. De esta forma, se dice

que esta firma es un concepto jurídico y un método de identificación, que se sirve de diversos soportes electrónicos, como un lápiz electrónico.

Las formas de firma electrónica son:

- Usando una firma biométrica.
- Firmando con un lápiz electrónico al usar una tarjeta de crédito o débito en un comercio.
- Marcando una casilla en una computadora, a máquina, o aplicada con el ratón o incluso con el dedo del usuario en una pantalla táctil.
- Usando una firma digital.
- Usando un sistema que obligue a establecer usuario y contraseña.
- Usando una tarjeta de coordenadas.

Una firma electrónica crea un historial de auditoría que incluye la verificación de quién envía el documento firmado y un sello con la fecha y hora" (Iprofesional, 2020, https://n9.cl/6wk98t).

Delitos informáticos y ciberseguridad

A continuación, se listan las normas principales que contemplan los delitos informáticos en la República Argentina. Te

recomendamos explorar cada una:

- Código Penal de La Nación Argentina Ley nro. 11.179: https://tinyurl.com/codigo-penal-arg.
- Ley nro. 26.388 de Delitos Informáticos: https://tinyurl.com/ley-26388-arg
- Ley nro. 27.411. Aprobación del Convenio sobre Ciberdelito (Convenio de Budapest sobre Ciberdelito): https://tinyurl.com/ley-27411-arg.
- Jefatura de Gabinete de Ministros (s.f.). *Normativa de Ciberseguridad*. https://n9.cl/hmzrh.
- Ministerio de Justicia (s.f.). Delitos Informáticos. https://n9.cl/qa4jr.

Ciberdelito

El Ministerio de Justicia y Derechos Humanos en su sitio web define al ciberdelito como "conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas. Son estafas, robo de datos personales, de información comercial estratégica, robo de identidad, fraudes informáticos, ataques como *cyberbulling*, grooming, phishing cometidos por ciberdelincuentes que actúan

en grupos o trabajan solos" (Carlos Felipe Law Firm, s.f., https://n9.cl/7r2kb6). La ciberdelincuencia está increíblemente organizada y profesionalizada.

Argentina tiene un marco normativo en ciberseguridad que incluye leyes como la de Delitos Informáticos (Ley nro. 26.388) y Ley de Protección de Datos Personales (Ley nro. 25.326), y recientemente, vía decreto a principios de 2026, se impulsó una **reforma de la Ley de Inteligencia Nacional** para separar la ciberseguridad de la ciberinteligencia, creando el **Centro Nacional de Ciberseguridad (CNC)**, autoridad de protección integral del ciberespacio. Esta disposición transformó la anterior Agencia Federal de Ciberseguridad en la **Agencia Federal de Ciberinteligencia (AFCI)**, enfocada en la obtención de inteligencia digital, alineando estas funciones bajo un sistema de inteligencia reorganizado.

Normativa clave preexistente:

- **Ley 26.388 (Delitos Informáticos):** Incorpora figuras penales como daño informático, fraude y violación de la privacidad.
- **Ley 25.326 (Protección de Datos Personales):** Regula el tratamiento de datos personales.

- **Ley 27.411 (Convenio de Budapest):** Adhesión al convenio internacional sobre ciberdelito.

- **Estrategia Nacional de Ciberseguridad (Res. 44/2023):** Establece lineamientos para la protección del ciberespacio nacional.

Reformas recientes (Decreto DNU 941/2025 - principios 2026):

- **Separación entre ciberseguridad/ciberinteligencia:** Define roles distintos para cada área.

- **Creación del Centro Nacional de Ciberseguridad (CNC):** Órgano rector de la protección integral del ciberespacio nacional, bajo Jefatura de Gabinete, encargado de la política y coordinación.

- **Agencia Federal de Ciberinteligencia (AFCI):** La antigua Agencia Federal de Ciberseguridad se convierte en AFCI, con foco en la producción de inteligencia en el ciberespacio.

- **Reorganización del Sistema de Inteligencia:** Se brinda mayor poder a la SIDE (ahora en proceso de reestructuración) y

redefinición de funciones para un sistema más moderno.

En resumen, Argentina está consolidando su marco legal, creando organismos específicos y separando competencias para abordar las amenazas digitales de manera más efectiva, mediante una ley de inteligencia nacional actualizada por decreto para el entorno digital.

Ejercicio para debatir

Luego de leer la normativa legal de nuestro país, se deja como ejercicio para los alumnos analizar a la luz de nuestra legislación, qué leyes podrían haber infringido lo realizado por Eduard Snowden.

CONTINUAR

Referencias

[Imagen sin título sobre algoritmo asimétrico] (2017) https://mundodelacomputacionbg.blogspot.com/2017/10/algoritmos-de-cifrado.html.

[Imagen sin título sobre algoritmo simétrico] (2017) https://mundodelacomputacionbg.blogspot.com/2017/10/algoritmos-de-cifrado.html.

Alfanumeric (s.f.). *Vectores de ataque en ciberseguridad*. Alfanumeric. https://www.alfa.com.ni/Post/Blog?Pid=03ec70fb-c430-4dd1-ae75-8458954a4e1e&Pid2=d4e3390e-f111-4ee0-866e-d205033fb6e9.

Baca Urbina, G. (2016). *Introducción a la seguridad informática*. México: Grupo Editorial Patria.

Educación IT (s.f.). *Ethical hacking: solucionar fallos de seguridad y prevenir la cibercriminalidad*. Educación IT. https://blog.educacionit.com/ethical-hacking-solucionar-fallos-de-seguridad-y-prevenir-la-cibercriminalidad/.

El Mundo (19 de diciembre de 2021). Log4Shell, el "fallo del siglo" que ha puesto a Internet de rodillas. *El Mundo*. https://www.elmundo.es/tecnologia/2021/12/19/61ba0ada21efa08f278b45f0.html

IONOS (2020). *Ethical hacking: solucionar fallos de seguridad y prevenir la cibercriminalidad*. IONOS. https://www.ionos.mx/digitalguide/servidores/seguridad/que-es-el-ethical-hacking/.

IONOS. (2017). *Penetration test (pentest): en qué consiste. IONOS. https://www.ionos.com/es-us/digitalguide/servidores/know-how/penetration-testing-la-verificacion-completa-para-tu-red/*.

López, A. (2025). *Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica*. Redes Zone. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/.

Lucena López, M. (2022). *Criptografía y Seguridad en Computadores*. Universidad de Vigo. https://ccia.esei.uvigo.es/docencia/SSI/cripto.pdf.

OSI. (28 de 08 de 2020). *¿Qué es una vulnerabilidad Zero Day?* OSI. https://www.osi.es/es/actualidad/blog/2020/08/28/que-es-una-vulnerabilidad-zero-day

Panelmega (s.f.). *Framework para pentester. Principales marcos para el pentesting*. Panelmega. https://panelmega.com/framework-para-pentester/.

Phil Zimmermann & Associates LLC (s.f.). *Philip Zimmermann creador de PGP*. Phil Zimmermann & Associates LLC. https://philzimmermann.com/ES/background/index.html.

Welle, D. (30 de 12 de 2013). *La NSA instaló programas espía en determinados ordenadores. DW*. https://www.dw.com/es/la-nsa-instal%C3%B3-programas-esp%C3%ADa-en-determinados-ordenadores/a-17333536

CONTINUAR

Lección 4 de 4

Descarga en PDF