Vulnerabilidades en sistemas operativos

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la bibliografía básica. Las definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha bibliografía.

El sistema operativo, en su rol de administrador de los recursos de un sistema, cumple un papel fundamental en la instrumentación de la seguridad de la información. En él convergen las vulnerabilidades propias de su diseño, las provenientes de la red y las que vienen de las aplicaciones que ejecuta, ya sea que se trate de aplicaciones propias o de componentes de *software* de terceros que lo integran y las introducidas por usuarios.

Se puede considerar a un sistema operativo como *seguro* en función de su arquitectura y las medidas de protección que implementa o bien en función del grado de cumplimiento que este ofrezca con respecto a la política de seguridad de la organización.

La protección proporcionada por sistemas operativos se entiende de forma básica como la *separación* entre usuarios. Esto significa separar los objetos de un usuario de los objetos de otros. Esta separación se puede lograr de distintas formas:

- Separación física: los procesos utilizan distintos objetos físicos.
- Separación temporal: procesos con diferentes requisitos de seguridad se ejecutan en tiempos distintos.
- Separación lógica: los usuarios operan como si no existiese otro proceso.
- Separación basada en uso de criptografía: los procesos protegen su entorno de ejecución y lo tornan ininteligible para el contexto externo.

Todas estas técnicas implican habilitar mecanismos que permitan cubrir varios objetivos en un sistema operativo:

- la protección de la memoria del sistema;
- la protección del sistema de archivos;
- el control de acceso a objetos generales;
- la autenticación de los usuarios;
- la ejecución bajo mínimos privilegios;
- la verificación de uso aceptable de los recursos del sistema.

Gran parte de estos mecanismos de seguridad se encuentran integrados en el *núcleo* del sistema operativo, mientras que otros se implementan de forma separada a través de soluciones *hardware* y *software*.

La elección entre soluciones *hardware* y soluciones *software* dependerá del subsistema que haya que proteger.

Entre estos subsistemas a proteger, se encuentran:

- la memoria;
- los dispositivos de entrada y salida;
- los programas compartidos;
- los datos compartidos en la red.

Se puede decir, entonces, que un sistema operativo seguro es aquel que proporciona las medidas de protección mencionadas, pero también de seguridad.

En el ámbito de los sistemas operativos, la definición de *protección* se puede establecer de forma complementaria con la definición de *seguridad*.

La *protección* supone el diseño de técnicas y mecanismos orientados a la protección del entorno de computación de un usuario frente a la intervención inadvertida o maliciosa de otros usuarios.

Sin embargo, la *seguridad* supone el diseño de aquellas técnicas y adopción de los modelos de funcionamiento que aseguran la confidencialidad, la integridad y la disponibilidad del sistema y de la información vinculada a este frente a amenazas externas.

Se puede concluir, entonces, que un sistema operativo *seguro* es un diseñado para garantizar cuatro aspectos fundamentales:

- La precisión funcional. El sistema operativo debe incorporar mecanismos diseñados para verificar que la ejecución de los procesos es tal y como se especificó en su fase de diseño.
  Esto supone habilitar la monitorización eficiente de procesos y un adecuado sistema de autoría de procesos.
- La integridad de la información y de las operaciones**.** La información que se genera e intercambia entre los procesos ejecutados por el sistema operativo no debe ser modificada por un elemento no autorizado. Debe incorporar mecanismos orientados a garantizar que sea imposible realizar este tipo de modificaciones no autorizadas y, en caso de que suceda, advertir su ocurrencia.
- La limitación de privilegios**.** El sistema operativo debe garantizar un adecuado control de acceso a los recursos del sistema.
- Nivel apropiado de confidencialidad. El sistema operativo debe implementar mecanismos que permitan adoptar esquemas complejos de confidencialidad.

Vulnerabilidades y ataques

Como se plantea en la introducción anterior, en el sistema operativo convergen las vulnerabilidades propias de su diseño y aquellas que hereda de la red, de las aplicaciones que ejecuta, de componentes de *software* de terceros que lo integran y las introducidas por usuarios o, mejor aún, las que hereda del *entorno* en el cual opera.

Si bien diversas bibliografías ofrecen listas prescriptivas de estas vulnerabilidades, cierto es que en la actualidad los esfuerzos y recursos destinados a vulnerar un sistema logran cierto grado de éxito, con lo cual estas listas se tornan insuficientes o adquieren una característica dinámica.

Como recurso alternativo, existen repositorios que documentan y catalogan a estas vulnerabilidades e incorporan además información útil para evaluar el nivel de riesgo que suponen y buenas prácticas para mitigarlas.

A continuación, se presentan de forma breve algunos de estos recursos.

National vulnerabilities database

Más conocido por las siglas NVD[1], se trata un repositorio proporcionado por el NIST (*National Institute of Standards and Technology*) en el que es posible consultar vulnerabilidades propias de sistemas operativos y otras aplicaciones *software*.

Cada vulnerabilidad es catalogada con un código **CVE**[2] (*common vulnerability exposure*). Este código CVE es utilizado cada vez más por fabricantes de herramientas de evaluación de seguridad para identificar vulnerabilidades y ofrecer de esta manera un vínculo al repositorio NVD, adonde analistas de seguridad y técnicos pueden obtener información detallada sobre el caso, el nivel de riesgo que supone, la criticidad y medidas para el tratamiento.

NVD introduce además una métrica de evaluación de vulnerabilidades conocida como *common vulnerability scoring system* (CVSS)[3], la que permite obtener una puntuación del impacto de una vulnerabilidad de acuerdo a sus características.

[1] Para más información sobre *national vulnerability database*, consulta: https://nvd.nist.gov/
[2] Para más información sobre *common vulnerabilities exposure*, consulta: http://cve.mitre.org/about/
[3] Para más información sobre *common vulnerabilities scoring system*, consulta: https://nvd.nist.gov/vuln-metrics/cvss

NVD ofrece además un panel de alertas e indicadores actualizados periódicamente que se puede utilizar como fuente de consulta permanente.

La figura que sigue ejemplifica una vulnerabilidad catalogada en el repositorio de NVD. Nótese su identificación bajo un código CVE, la descripción resumida, que puede ser profundizada al ingresar al seleccionar el código CVE, las métricas de impacto obtenidas con los métodos CVSS y otra información de interés como la fecha de publicación.

Figura 1: Ejemplo de vulnerabilidad catalogada en NVD

Fuente: National vulnerability database, 2017, https://goo.gl/dz9wvk.

Common weakness enumeration

Conocido comúnmente por sus siglas en inglés CWE[4], es una iniciativa de The MITRE Corportation [5] y su repositorio se encarga agrupar por tipo a las distintas *debilidades* identificadas en *software*. Cada tipificación es identificada por un código CWE e ingresada al repositorio con información detallada.

Este repositorio se encuentra disponible para consultas web y también en formatos para descarga como .XML, texto o .PDF.

MITRE es además el creador de CVE. La diferencia entre CWE y CVE radica en que una debilidad (*weak*) expone a una serie de vulnerabilidades (*vulnerabilities*), con lo cual se puede pensar en CWE como un agrupamiento o categorización de CVE y, por lo tanto, es posible relacionarlos a través de un esquema jerárquico.

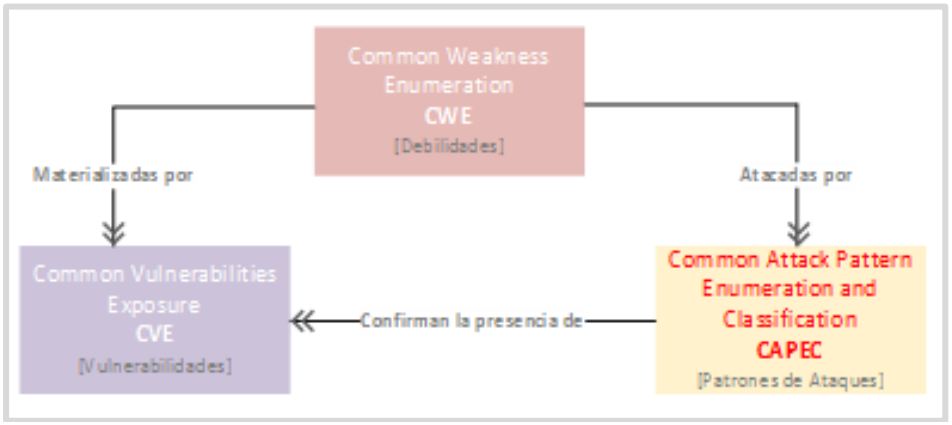
CWE ofrece una metodología para puntuación de debilidades conocida como *common weakness scoring system* (CWSS)[6] y una metodología para

[4] Para más información sobre *common weakness enumeration*, consulta: http://cwe.mitre.org/index.html
[5] Para más información sobre MITRE, consulta: https://www.mitre.org/
[6] Para más información sobre *common weakness scoring system*, consulta: http://cwe.mitre.org/cwss/cwss_v1.0.1.html

evaluación de riesgos *common weakness risk analysis framework* (CWRAF)[7].

Otra herramienta útil que provee MITRE es el catálogo de patrones de ataques *common attack pattern enumeration and classification* (CAPEC)[8], cuyo objetivo es proporcionar un catálogo de patrones de ataque comunes clasificados de una manera intuitiva.

Figura 2: Esquema CWE y su relación con otros catálogos



Fuente: adaptación propia con base en University of Nebraska Omaha, 2017.

Open web application security project

Ampliamente reconocido por sus siglas OWASP[9], se trata de un proyecto colaborativo que provee catálogo documentado de vulnerabilidades, principalmente relacionadas con aplicaciones web.

OWASP provee también metodologías de desarrollo seguro de *software*, herramientas de análisis de código fuente, evaluación de vulnerabilidades, entre otras soluciones relacionadas con la seguridad de aplicaciones.

Un recurso muy conocido es el reporte *OWASP Top 10 Application Security Risks*[10]*, el* que se publica con frecuencia. En él, se listan a modo de *ranking* las vulnerabilidades más comunes encontradas en aplicaciones.

[7] Para más información sobre *common weakness risk analysis framework*, consulta: http://cwe.mitre.org/cwraf/
[8] Para más información sobre *common attack pattern enumeration and classification* consulta: http://capec.mitre.org/about/index.html
[9] Para más información sobre *open web application security project*,: https://www.owasp.org
[10] Para más información acerca de OWASP Top 10, consulta: https://www.owasp.org/index.php/Top_10_2017-Top_10

En resumen, la seguridad de los sistemas operativos reside tanto en su diseño como en factores externos a este. Los principales mecanismos de seguridad se encuentran implementados a nivel del núcleo del sistema operativo y son complementados por componentes *hardware* y *software*.

Para catalogar a un sistema operativo como seguro, no es suficiente que asegure la confidencialidad, integridad y disponibilidad de la información que procesan y almacenan, sino que además debe proveer mecanismos que aseguren la precisión de las funcionalidades que incorpora y la ejecución bajo los privilegios adecuados.

Por otro lado, la caracterización de sistema operativo seguro o inseguro puede ser determinada en función del grado de cumplimiento de los requisitos de seguridad emanados de la política de seguridad de la información de la organización.

En relación con las vulnerabilidades y ataques a los que se encuentran expuestos los sistemas operativos, los catálogos disponibles en línea son un excelente recurso útil como fuente de consulta, ya que se mantienen listas actualizadas, entre otras herramientas.

Referencias

Deitel, H. M. (1987). *Introducción a los sistemas operativos*. México: Addison-Wesley Iberoamericana.

Echaiz, J. (2002). Protección en sistemas operativos 1. Recuperado de www.ing.unp.edu.ar/asignaturas/seminarioseguridad/ProtOS-%201.ppt

Gómez Vieites, A. (2011). *Enciclopedia de la seguridad informática* (2.ª ed.). Madrid, España: Ra-Ma.

La Red Martínez, D. (2015). *Seguridad de los sistemas operativos*. Recuperado de http://exa.unne.edu.ar/informatica/SO/SO14.htm#Intro

National Vulnerability Database. (2017*). CVE-2017-0211*. Recuperado de https://nvd.nist.gov/vuln/detail/CVE-2017-0211

University of Nebraska Omaha. (2017). *Software Assurance* (Traducción propia). Recuperado de https://robinagandhi.github.io/swa/slides/lecture-5/code-for-software-se.html#48

Administración segura de servidores

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la bibliografía básica. Las definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha bibliografía.

Los servicios provistos dentro de una infraestructura de tecnología residen en amplia mayoría en los servidores.

Así, en una red LAN (red de área local, en español) de una organización, se pueden encontrar servidores dedicados al servicio de correo electrónico, servidores de archivos, servidores de servicios web, servidores de copias de seguridad, servidores de *software* de negocio, servidores de escritorio remito, entre otros.

Dado que tienen relación directa con la operatividad de la organización en algunos casos, y en otros procesan y almacenan información sensible, es necesario y fundamental dotarlos de seguridad. Para ello, se utiliza el concepto de *hardering* del sistema, que se refiere a extremar la implementación de medidas y mecanismos de protección, sea sobre un equipo servidor o una estación de trabajo cualquiera perteneciente al contexto de la organización.

Como en todos los ámbitos de la seguridad, este *hardering* no puede basarse en medidas arbitrarias, sino que debe seguir buenas prácticas de configuración segura y, por otro lado, debe basarse en la política de seguridad de la información de la organización.

Administración segura de servidores

Generalmente, los fabricantes de *softwares* proveen sus productos con configuraciones generalizadas de manera que estas se adapten a cualquier entorno en el que se instalen y se facilite el proceso de instalación y puesta en producción. Esto provoca que en las instalaciones iniciales existan cuentas de usuarios por defecto, numerosos servicios en ejecución y componentes que, de acuerdo con el escenario, pueden o no ser necesarios. Se parte de una base cuya premisa indica que *lo que no está expresamente prohibido, está permitido* con el foco puesto sobre la operatividad y no la seguridad.

El punto de partida hacia una administración segura de servidores es establecer la premisa inversa: *todo lo que no está expresamente permitido, está prohibido*.

Ahora bien, para determinar lo que está *expresamente permitido* se debe recurrir en primera instancia a la política de seguridad de la organización y extraer de ella los requerimientos de seguridad que demande. En segunda

instancia, se debe recurrir a guías de buenas prácticas de configuración segura que servirán de marco para complementar todas las características de seguridad que se deberán aplicar sobre el servidor.

Es común que en ciertos casos se presenten conflictos entre lo que especifique una guía de configuración frente a los requisitos de seguridad de la política de seguridad. En estos casos, debe prevalecer la necesidad del negocio y se debe documentar la no aplicación de la buena práctica con su respectiva justificación.

Una vez identificados todos los requisitos y características de seguridad que deben ser aplicadas, se deben elaborar los estándares de configuración propios de la organización.

Algunas de las guías de configuración segura surgen de las normativas estándares ya comentadas en lecturas anteriores y que se citan a continuación:

- ISO 27001:2013[1]. Tecnologías de información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requerimientos.
- ISO 27002:2009[2]. Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.
- PCI DSS versión 3.2[3]. *Data security standard*.
- NIST SP 800-70 Rev. 3[4]. *National checklist program*.

A modo de ejemplo, se deberán elaborar algunos de los siguientes documentos:

- Estándar de configuración para sistemas operativos Windows Server.
- Estándar de configuración para servidores web basados en internet información *server*.
- Estándar de configuración para servidores Ubuntu Server.

Documentación de un estándar de configuración segura

A continuación, se desarrolla, a modo de ejemplo, un estándar de configuración segura para servidores basados en Microsoft Windows Server.

[1] ISO/IEC 27001 tecnologías de Información. Técnicas de seguridad. Sistemas de seguridad de la Información. Requisitos. Recuperado de https://www.iso.org/standard/54533.html
[2] ISO/IEC 27002 Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. Recuperado de https://www.iso.org/standard/54533.html
[3] PCI *data security standard*. Recuperado de https://es.pcisecuritystandards.org/minisite/env2/
[4] *National checklist program for IT products*: *guidelines for checklist users and developers*. Recuperado de http://csrc.nist.gov/publications/drafts/800-70/sp800-70r3_draft.pdf.

1) Introducción

El presente estándar define los términos y procedimientos para una configuración adecuada y segura de servidores basados en Windows Server de la empresa Muy Segura S. A.

2) Objetivo

El objetivo del presente estándar es proporcionar a los administradores de sistemas, personal de TI (tecnologías de la información) u otro personal habilitado la información apropiada para cumplir con la política de seguridad aplicada a la configuración de un servidor basado en Windows Server, tendientes a alcanzar un uso seguro y confiable.

3) Alcance

El presente estándar aplica exclusivamente a los servidores basados en sistema operativo Windows Server de la empresa Muy Segura S. A.

4) Estándar

4.1 Requerimientos de servidores

Antes de cualquier instalación de un servidor Windows Server, se debe confeccionar y aprobar por la dirección un formulario de solicitud que especifique y fundamente la necesidad de este.

4.2 Guía de configuración

Se deberán aplicar las siguientes configuraciones:

4.2.1 Se deberán instalar versiones de Windows Server 2012 exclusivamente.
4.2.2 Se deberá modificar la clave del usuario administrador por una clave segura basada en el estándar de claves seguras de la empresa.
4.2.3 Se deberá unir el servidor al dominio de la empresa.
4.2.4 Se deberá utilizar exclusivamente el sistema de archivos NTFS (New Technology File System)

4.3 Herramientas de seguridad

Se deberán instalar, configurar y dejar en ejecución las siguientes herramientas de seguridad:

4.3.1 Antivirus, *antimalware* e IDS (Intrusion Detection System) definidos en el estándar de herramientas de seguridad de la empresa.

4.4 Información a otras áreas

Se deberá informar a las áreas y responsables involucrados en caso de que el servidor requiera configuraciones adicionales.

4.4.1 Notificar al responsable de las copias de seguridad para que incluya al servidor dentro de las rutinas de copias de seguridad.
4.4.2 Notificar al responsable de red para que aplique las políticas de ruteo definidas en la política de red de la empresa.

5) Definiciones
5.1 Servidor: a los efectos de la presente política, un servidor es un equipo destinado a proveer servicios de información en el contexto de la empresa Muy Segura S. A.

6) Historial de revisiones
01/04/2017: redacción borrador. Responsable: Juan Pérez.

Monitorización de eventos

La monitorización de eventos es una de las herramientas de seguridad elementales que debe disponer un servidor y fuente de información permanente para la organización en relación al de estado de la seguridad de su infraestructura.

En líneas generales, todo sistema operativo de servidor implementa un registro de eventos y ofrece una herramienta de consultas.

Cuando la cantidad de servidores que integran una infraestructura es importante, la monitorización se torna ineficiente si no se cuenta con un único punto de consulta.

Entre las soluciones que ayudan a resolver esta problemática, se encuentra el protocolo simple de administración de red, más conocido como SNMP (Simple Network Management Protocol) por sus siglas en inglés. SNMP puede operar como agente en un dispositivo de red o servidor y enviar los eventos a un repositorio común.

Los sistemas de detección de intrusión implementan la misma capacidad que ofrece SNMP, aunque incorporan además funciones de proactivas de seguridad.

Otras soluciones más avanzadas como los sistemas de correlación de eventos SIEM (Security information and event management) despliegan

agentes de recolección de eventos a través de la red para recuperar información de eventos. Estos eventos son almacenados y analizados en busca de patrones de comportamientos no autorizados.

Figura 1: Panel de información de herramienta SIEM AlienVault

Fuente: adaptación propia con base en AlientVault, 2017.

En resumen, la protección de servidores es una tarea que requiere de una instancia de planificación en la que se reúnen los requisitos y características de seguridad que serán implementados. Estos requisitos de seguridad surgen tanto de la política de seguridad de la organización como de las guías de buenas prácticas de configuración segura. Esta última no es de libre elección, sino que la organización debe definir cuáles normativas estándares están alineadas con los objetivos de negocio y que serán empleadas como marco de referencia.

Se debe documentar en formato de estándares de configuración segura cada tipo de instalación de servidor, con el objetivo de conformar un repositorio que sirva de referencia para necesidades futuras con el fin de mantener instalaciones de servidores homogéneas.

La monitorización de eventos, como se planteó, es un aspecto elemental que sirve de base para la evaluación del estado de seguridad de la infraestructura y servirá también como fuente de análisis y evidencias ante determinados eventos no autorizados.

Para una administración eficiente de los registros de eventos, se deben implementar repositorios centralizados que sirvan de único punto de consulta, utilizando para el protocolo SNMP u otras soluciones basadas en recolección y administración de eventos.

Referencias

AlienVault. (2017). Panel de información de herramienta SIEM [Imagen]. Recuperado de http://i.imgur.com/aIqRaKZ.png

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática* (2.ª ed.). Madrid, España: Ra-Ma.

ISO/IEC 27001. (2013a). [Tecnologías de información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requerimientos]. Suiza: Organización Internacional de Estandarización (ISO). Recuperado de https://www.iso.org/standard/54534.html.

ISO/IEC 27002. (2013b). [Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información]. Suiza: ISO. Recuperado de https://www.iso.org/standard/54533.html.

PCI DSS v.3.2. (2016). [Data Security Standard]. Massachusetts: Payment Card Industry Security Standards Council. Recuperado de https://es.pcisecuritystandards.org/minisite/env2/

SP 800-70. (2015). [National Checklist for IT Products: Guidelines for Checklist Users and Developers]. Estados Unidos: National Institute of Standards and Technology Special. Recuperado de http://csrc.nist.gov/publications/drafts/800-70/sp800-70r3_draft.pdf.

Tecnologías de control de acceso

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la bibliografía básica. Las definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha bibliografía.

Las tecnologías de control de acceso son la primera línea de defensa para la seguridad de la información de la organización.

Esta lectura revisa la protección de la información mediante técnicas que permiten a los usuarios presentar una identidad a un sistema y probarlo de algún modo (autenticación) para que, posteriormente, utilicen el sistema de manera limitada de acuerdo con el establecimiento de qué pueden hacer con qué recursos (autorización). Además, se presenta una revisión sobre los principales aspectos en relación con la cuentas de usuarios y gestión de claves.

Cuando se producen intrusiones o accesos indebidos, el sistema debe estar preparado para proporcionar una traza fiable de las acciones de los usuarios (*accountability*) para identificar el problema y las responsabilidades.

Tecnologías de control de acceso

El control de accesos es el conjunto de mecanismos y procedimientos que permiten a los gestores de la seguridad controlar y restringir el uso de los recursos del sistema de información y el comportamiento de los usuarios en relación con este. Particularmente, se trata de controlar:

- qué pueden hacer los usuarios en el sistema;
- a qué recursos del sistema pueden acceder;
- qué operaciones pueden realizar con esos recursos.

Este dominio de la seguridad se basa fundamentalmente en la *confidencialidad* mediante el control de quién accede a qué información.

No obstante, la *integridad* solo se puede garantizar si el control de accesos asegura la *integridad de los datos*, esto es que los datos sean fieles a la información que deben reflejar y la *integridad del sistema*, es decir, que se comporte como se espera. Desde una perspectiva diferente, el control de accesos debe garantizar la *disponibilidad* del acceso de los usuarios autorizados de acuerdo con los usos legítimos del sistema y de la información.

Se considera que el control de accesos es la primera línea de defensa de seguridad. El control de accesos afecta tanto a los accesos físicos como a los accesos por vía informática.

Triple *A* del control de acceso

La función del control de accesos se puede resumir en la ***triple A***, que proviene de los siguientes términos en inglés:

- *Authentication:* Antes de que un usuario pueda acceder al sistema, debe haber sido autenticado, es decir, su identidad debe haber sido comprobada.
- *Authorization*: Para los usuarios legítimos, el acceso a los recursos debe provenir de una autorización explícita y reconocible de usos legítimos.
- *Accountability*: El sistema debe permitir conocer las acciones de los usuarios en el sistema para comprobar *a posteriori* que los usos han sido los autorizados.

El control de accesos se basa en dos principios fundamentales:

  - *La separación de responsabilidades*. Implica que, para cada tarea, se separan los diferentes pasos y estos deben ser realizados por personas diferentes.
    Para lograrlo, primero hay que definir los elementos de cada proceso o función de trabajo. Una vez hecho esto, los elementos definidos se dividen entre los diferentes usuarios. Esto evita que un individuo tenga control de un proceso y, lo por tanto, la capacidad de manipular el proceso para obtener beneficios personales. Visto desde otra perspectiva, implica que, para cometer un fraude, al menos hace falta el acuerdo de dos personas.
  - *Mínimos privilegios*. Establece que solo se debe autorizar a un usuario aquellos recursos de información y operaciones sobre ellos que sean imprescindibles para su trabajo.

Ambos principios se deben combinar con la clasificación de la información para configurar un mapa de autorizaciones.

Mecanismos de autenticación

La identificación de un usuario es el proceso por el cual este presenta una identidad concreta. La autenticación es el proceso de proporcionar alguna prueba o pruebas de que esa afirmación es verdadera.

La autenticación se basa en alguno o en combinación de los siguientes factores:

- Algo que el usuario conoce. Por ejemplo, se asume que solo el usuario conoce su palabra clave, el PIN (número de identificación personal, en inglés) o la respuesta a una pregunta relacionada con su vida privada.
- Algo que el usuario posee. Por ejemplo, se supone que solo el usuario posee su tarjeta de identificación.
- Algo que el usuario es**.** En este caso, se reconoce alguna característica física del usuario. Este tipo agrupa las técnicas biométricas, como el reconocimiento de huellas dactilares, los escáneres de retina o el reconocimiento de patrones de voz.

En la siguiente tabla, se presentan algunas de las tecnologías utilizadas para la autenticación de usuarios.

Tabla 1: Tecnologías de autenticación

Tecnología	Información
Técnicas biométricas	La biometría se refiere a la identificación automática de una persona según sus características fisiológicas o de comportamiento. Ejemplos: huella dactilar, reconocimiento facial, información del iris.
Técnicas SSO (*single sign on*)	Se trata de un control de acceso coordinado para varios sistemas *software* independiente entre sí. Con SSO, un usuario inicia sesión una vez y le sirve para todos los sistemas sin que se le pida que se autentique de nuevo en cada uno de ellos.
Kerberos	Es un protocolo diseñado para proporcionar autenticación fiable en redes abiertas e inseguras, donde las comunicaciones entre los equipos que pertenecen a esta pueden ser interceptadas. Fue diseñado e implementado a mediados de 1980 por el Instituto de Tecnología de Massachusetts (MIT). Utiliza criptografía de clave simétrica.
Secure european system for applications in a multi-vendor environment (SESAME)	Permite el acceso basados en roles, por lo que posibilita la autorización junto con servicios de autenticación. También es compatible con el concepto de delegación de privilegios de un usuario a otro usuario o aplicación. Se basa en criptografía de clave pública.

Fuente: elaboración propia.

Mecanismos de autorización

Los mecanismos de autorización son métodos diseñados para la autorización del acceso a recursos al seguir determinadas reglas. Estos mecanismos se han desarrollado en diferentes entornos, comenzando por los propios sistemas operativos y bases de datos.

En la siguiente tabla, se presentan los métodos utilizados para la autenticación de usuarios.

Tabla 2: Tecnologías de autenticación

Tecnología	Información
Discrecional DAC	*Discretionary access control*. Medio para restringir el acceso a los objetos en función de la identidad de los usuarios o grupos a los que pertenecen. Los controles son discrecionales en el sentido de que un usuario con un permiso de acceso es capaz de transmitir ese permiso.
Obligatorio MAC	*Mandatory access control*. La política de seguridad está controlada por un administrador y los usuarios no tienen la capacidad de anular la política. Algunos sistemas operativos como Secure-Enhanced Linux (SELinux) o Windows Vista con el denominado *mandatory integrity control* (MIC) incorporan mecanismos MAC en lugar de DAC.
Basado en roles (RBAC)	*Role-Based Access Control*. Se basa en la idea de asignar los permisos a roles predefinidos y no a los usuarios directamente. Esto hace más fácil la gestión de los permisos, dado que hay un proceso de clasificación previa de los niveles de acceso que se materializa en roles, que pueden relacionarse en jerarquías y formar árboles o, más en general, grafos. Las aplicaciones (*subject*) o usuarios se asignan a roles determinados, y son estos roles los que tienen asociados ciertos permisos sobre ciertas operaciones.

Fuente: elaboración propia.

Mecanismos de registro y auditoría de accesos

La contabilidad (*accountability*) hace referencia a la posibilidad de registrar las sesiones y transacciones de los usuarios del sistema con el objetivo de

obtener información de estos con propósitos de auditoría de seguridad. Actualmente, se suele hablar de *auditoría* como término más general, que incluye la contabilidad.

Un aspecto fundamental de esta auditoría es el mantenimiento de repositorios o registros de transacciones (*logs*) y, lógicamente, el que esos repositorios no puedan alterarse o ser accedidos por usuarios no legítimos. No obstante, los *logs* son una colección de documentos que no producen ninguna información valiosa *per se*, sino solamente cuando se someten a procesos de revisión periódica con el objeto de detectar intrusiones o usos no legítimos.

Tecnologías triple *A*

En seguridad de la información, AAA es sinónimo de *autenticación, autorización y contabilidad*, términos que provienen de su traducción del inglés. AAA hace referencia a una arquitectura de seguridad para sistemas distribuidos que permite el control sobre a qué usuarios se les permite el acceso a los servicios y la cantidad de los recursos que han utilizado.

En la siguiente tabla, se mencionan tres de los protocolos más implementados y que se encuentran detallados en la bibliografía básica.

Tabla 3: Principales tecnologías triple *A*

Tecnología	RADIUS	Diamenter	TACACS+
Especificación	RFC 2865[1]	RFC 6733[2]	Propietario, CISCO[3]
Protocolo	Basado en UDP	Basado en TCP	Basado en TCP
Características	AAA consolidado	Evolución de RADIUS con mejoras en la fiabilidad y escalabilidad	AAA se implementa como funciones separadas
Protección	Solo credenciales de usuario	Se basa en IPSec o TLS	Protege todos los datos de AAA

Fuente: elaboración propia.

[1] *Remote authentication dial in user service* (RADIUS): https://tools.ietf.org/html/rfc2865
[2] *Diameter base protocol*: https://tools.ietf.org/html/rfc6733
[3] *Terminal access controller access control system*: https://es.wikipedia.org/wiki/TACACS

Cuentas de usuarios y gestión de claves

Todos los aspectos relacionados con las cuentas de usuarios y gestión de claves deben estar claramente definidos y gestionados a través de las políticas de seguridad de la organización. En ellas, se deben especificar aspectos como características de contraseñas seguras, caducidad de las contraseñas, nomenclaturas para asignación de cuentas de usuarios, entre otros.

La delimitación de responsabilidades es otro de los aspectos que se deben considerar. Los usuarios deben ser conscientes de que deberán rendir cuentas de toda actividad realizada en su nombre, incluso cuando dichas actividades hayan sido realizadas en un marco de suplantación de identidad. La seguridad de sus credenciales depende del uso responsable de esta.

Es importante que cualquier definición de política relacionada con los usuarios se encuentre alineada con los normativas legales vigentes. Es una buena práctica acordar con los usuarios convenios de confidencialidad y uso responsable que englobe estos y otros temas que lo involucren.

En resumen, el control de acceso es uno de los principales mecanismos de protección de seguridad de la información en el contexto de una organización. La autenticación, autorización y contabilidad o registro de accesos brindan información elemental para la gestión de seguridad de los activos de información.

A través del control de acceso, se puede lograr la confidencialidad y la integridad de la información. Distintos métodos y tecnologías permiten la implementación de controles de acceso más o menos robustos que serán adoptados en función de las necesidades del contexto en el que se implementen.

Es importante tener en cuenta que el control de acceso abordado tiene que ver con la seguridad lógica del sistema. En un contexto organizacional, este tipo de seguridad debe ser complementada también con seguridad física del entorno. La una sin la otra no es suficiente para cubrir el amplio espectro que suponen las vulnerabilidades.

La gestión de claves y cuentas de usuario implica un control administrativo que debe ser abordado desde la política de seguridad de la información de la organización, sin perder de vista los lineamientos legales o jurídicos que apliquen, dado que existe una proximidad con temas inherentes a la privacidad.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la seguridad informática* (2° ed.) Madrid, España: Ra-Ma.

Aspectos legales y regulatorios

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la bibliografía básica. Las definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha bibliografía.

Los aspectos legales y regulatorios que subyacen en relación con las nuevas tecnologías de información y comunicaciones tienen un impacto relevante sobre estas, pues definen el marco jurídico del entorno sobre el cual estas deben operar.

Identificar los riesgos legales a los que puede exponerse un proyecto es una tarea relevante en el marco de la seguridad de la información. Esta considera, por ejemplo, que en un proyecto de *software* se utilizan componentes protegidos por derechos de autor, cuya potestad que no se ha tenido en cuenta. Esos derechos pueden ser reclamados en un futuro, lo cual comprometerá a todos los involucrados tanto en el desarrollo como en el uso del producto desarrollado. Más aún, aquel conjunto normativo considera cómo proceder si en dicho proyecto se pasan por alto las normas aplicables a la recolección de datos personales, lo que puede resultar en litigios con los usuarios o clientes por la vulneración de su privacidad. Claramente, son escenarios que deben ser evaluados y abordados conforme a los lineamientos jurídicos aplicables.

En la presente lectura, se revisan los principales aspectos que se deben tener en cuenta en los términos de propiedad intelectual, licenciamiento de software, contratos electrónicos y protección de datos personales.

Propiedad intelectual

La propiedad es una institución tan antigua como el ser humano. Desde las primeras sociedades, la propiedad existe, esencialmente sobre objetos materiales. La ganadería, el cultivo, la tierra, la producción y sus excedentes son solo algunos ejemplos de bienes materiales objetos de apropiación.

Actualmente, la propiedad es uno de los institutos jurídicos sobre los que se asienta cualquier sociedad moderna; en el caso argentino, es un derecho, reconocido por la Constitución Nacional: “Artículo 14. Todos los habitantes de la Nación gozan de los siguientes derechos… de usar y disponer de su propiedad...”[1]. Este mismo documento declara:

> Artículo 17. La propiedad es inviolable y ningún habitante de la Nación puede ser privado de ella, sino en virtud de

1 Art. 14, Ley 24.430. (1994). Constitución Nacional Argentina. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/6tYK6J

> sentencia fundada en ley… Todo autor o inventor es propietario exclusivo de su obra, invento o descubrimiento, por el término que le acuerde la ley.[2]

De la misma forma que sucede con los bienes materiales, los bienes inmateriales existen ante la ley, e igualmente los derechos de propiedad sobre ellos, los que son tutelados desde las primeras sociedades humanas organizadas. Los bienes inmateriales, especialmente el conocimiento, son tan antiguos como la capacidad del hombre de innovar, y tienen, actualmente, en la sociedad del conocimiento, una alta relevancia económica; por ende, su caracterización económica es también relevante.

Las tecnologías de información y las comunicaciones constituyen un sector importante en la creación de conocimiento, esto es, de bienes inmateriales o intangibles, entre los cuales uno de los casos más paradigmáticos es el software.

La vía esencial para la protección jurídica de los bienes inmateriales son los denominados **derechos de propiedad intelectual**, que en el caso argentino son tutelados por la **Ley 11.723**[3], y **materializados a través de los derechos de autor**.

Para dotar de un marco jurídico al software, dado que, al momento de promulgación de la citada ley de propiedad intelectual, este aún se encontraba en sus fases iniciales, se introdujo una reforma por medio de la **Ley 25.036**[4], cuyo artículo primero lo cita en un listado enunciativo:

> Artículo 1º - A los efectos de la presente ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, **entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales**;… sea cual fuere el procedimiento de reproducción.[5]

2 Art. 17, Constitución Nacional Argentina. (1994). [Aprobada por Ley 24.430]. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/6tYK6J
3 Ley 11.723. (1933). Régimen Legal de Propiedad Intelectual. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/VNFmHa
4 Ley 25.036. (1998). Propiedad Intelectual [Modificatoria de la Ley 11.723, Régimen Legal de la Propiedad Intelectual]. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/6Vo2Yx
5 Art. 1, Ley 25.036. (1998). Propiedad Intelectual [Modificatoria de la Ley 11.723, Régimen Legal de la Propiedad Intelectual]. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/6Vo2Yx

Con esta reforma a la ley de propiedad intelectual, se incorporaron herramientas que protegen al software contra los diversos ataques que puedan presentarse en torno a la reproducción, venta, edición, falsificación o uso sin autorización.

En Argentina, el órgano de control de los derechos de autor es la **Dirección Nacional de Derechos de Autor**[6], dependiente del Ministerio de Justicia y Derechos Humanos de la Nación. Entre sus competencias, se encuentra el **registro de software**.

Licenciamiento de software

Si el medio para proteger la propiedad del software es el marco jurídico de la propiedad intelectual, materializado a través del derecho de autor, la licencia es el vehículo para la transmisión de derechos de sobre este.

La ley argentina de propiedad intelectual establece que "la explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencia para su uso o reproducción"[7]. Estas licencias pueden clasificarse por amplitud o cantidad de derechos que conceden al usuario. Típicamente hay tres grandes grupos de licencias:

1) Licencias sobre el software propietario

Se trata de un contrato de adhesión, o de licencia de uso, entre el fabricante o autor del software y el usuario final de este, en el cual se fija el régimen jurídico en términos de derechos y obligaciones o restricciones del usuario sobre el producto licenciado.

El propietario cede su uso al adquirente, sin que llegue a trasmitirle la propiedad de este, y ello a cambio del pago de los denominados derechos de licencia.

2) Licencias del modelo de software libre

Se trata de un modelo o, más bien, de un movimiento, dado que sus fundamentos son más filosóficos que comerciales, que tuvo su origen

6 Véase la web de la Dirección Nacional de Derechos de Autor, Ministerio de Justicia y Derechos Humanos, ingresando en https://goo.gl/zfZzgz

7 Art. 55 bis, Ley 11.723. (1933). Régimen Legal de Propiedad Intelectual. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/VNFmHa

en la década de los años 80 con el denominado proyecto GNU (cuyo acrónimo significa GNU No es Unix), liderado por Richard Stallman[8].

Estas licencias son auspiciadas por la Fundación de Software Libre (FSF)[9], cuyo objetivo es eliminar las restricciones sobre el copiado, redistribución, entendimiento y modificación de software, promocionando así el desarrollo y uso del software libre en todas las áreas de la computación.

Este tipo de licencias confieren a los usuarios las siguientes libertades:

- libertad de uso del programa, con cualquier propósito;
- libertad de estudiar su funcionamiento y adaptarlo a las necesidades, con el otorgamiento del acceso al código fuente como condición previa para ello;
- libertad de distribuir copias;
- libertad de mejorar el software y hacer públicas dichas mejoras, como un medio para beneficiar a la comunidad (Barbosa Ruiz y Alfaro Arriola, 2013).

Para evitar que el software licenciado bajo este esquema sea utilizado como base para el desarrollo de software propietario, se creó el concepto ***copyleft***[10], que consiste en un medio legal que implica que cualquier versión modificada del software derivado hereda el mismo tipo de obligaciones y derechos que tiene el software original. Cualquier software derivado debe brindar, a la vez, las cuatro libertades comentadas anteriormente. En síntesis, el objetivo del copyleft es garantizar que cualquier software derivado continúe otorgando a los usuarios las mismas libertades que confiere el software original.

Las licencias más extendidas de este tipo son la **General Public Licence (GPL)**[11] y **Lesser-GPL**[12]. En ambos casos, se exige detallar las modificaciones introducidas en el software original y el autor de dichas modificaciones. Además, se incluyen cláusulas que limitan la responsabilidad, susceptible de modificación, que solo afectarán al distribuidor o el desarrollador final.

8 Véase más información sobre el proyecto GNU (1984) ingresando en https://goo.gl/wn1a52
9 Véase más información sobre la Free Software Foundation ingresando en https://goo.gl/kH5FN
10 Véase más información sobre copyleft ingresando en https://goo.gl/5ByiEB
11 Véase más información sobre la General Public Licence (GPL) ingresando en https://goo.gl/7DwX1
12 Véase más información sobre la Lesser General Public Licence (LGPL) ingresando en https://goo.gl/imgtz

Por último, cualquiera de estas dos licencias prevé cláusulas de excepción de responsabilidad y negación de garantía; a pesar de esto, el posterior desarrollador o distribuidor cuenta con libertad para asumir mayores obligaciones al respecto.

3) Licencias del modelo de software de código abierto

Este modelo de licencia toma como base las ventajas que aporta a la comunidad el código abierto; sin embargo, presenta diferencias bien marcadas con respecto al modelo de software libre en lo que hace a su enfoque. El movimiento Open Source parte de una motivación pragmática: ve la excelencia técnica y la garantía de las cuatro libertades que sustentan la filosofía del software libre como los objetivos prioritarios, y, en definitiva, compartir el código fuente es un medio para alcanzar dicho fin. En otras palabras, el movimiento del software libre hace especial énfasis en los aspectos morales o éticos del software, es decir que la excelencia técnica es un resultado derivado de su estándar ético, cuyas cuatro libertades constituyen un fin en sí mismas.

Las licencias correspondientes al modelo de software de código abierto se caracterizan por conceder al usuario **disponibilidad absoluta sobre el software, ya que brindan un acceso total a su código fuente**; además y contrariamente al modelo anterior, **no obligan a que el software derivado mantenga condición alguna en cuanto a la apertura o no de su código**.

Este tipo de licencias permiten al usuario **copiar, usar, distribuir y modificar el código libremente**, imponiendo mínimas condiciones, tales como la incorporación de información relacionada al *copyright* del desarrollador inicial y participantes, la prohibición de hacer uso del nombre de estos para garantizar o promocionar el software generado en desarrollos posteriores, y la incorporación de una cláusula de exención de responsabilidad en relación a los primeros. De todas maneras, ninguna de estas condiciones impide que el desarrollador final asuma mayores responsabilidades ni que extienda garantías sobre su producto.

En síntesis, este modelo de licenciamiento de código abierto permite la posibilidad de crear un software propietario tomando como base un software de código abierto.

La licencia más extendida de este tipo es la Berkeley Software Distribution (BSD)[13]. Esta se destaca por ser la licencia existente con mayor grado de permisividad: habilita el uso con cualquier finalidad, permite la modificación y creación de software derivado y su distribución, ya sea como software libre o de código abierto, o bien como software propietario, siempre y cuando los ejemplares incluyan un tipo determinado de licencia, además de un aviso sobre el derecho de autor, un descargo de garantía y una limitación de responsabilidades.

Por último, volviendo al marco normativo, se debe que tener presente que en el fondo de estos modelos de licenciamiento reside un contrato, y las generales de aplicabilidad estarán además sujetas al marco jurídico del país que se designe como sitio de litigio de las diferencias que se presenten.

Contratos informáticos

Un contrato es un acuerdo entre partes para realizar un intercambio de bienes o servicios de carácter patrimonial, es decir, susceptibles de valoración económica.

Llevado este concepto al campo de la informática, se puede decir que un Contrato Informático es una contratación cuyo objeto son bienes y servicios informáticos.

Por consiguiente, los objetos involucrados en los acuerdos de carácter patrimonial entre personas (físicas o jurídicas) son:

1. Bienes informáticos. Con una doble tipología:

- **Elementos tangibles de un sistema informático.** Todos aquellos dispositivos que forman la parte física del sistema, lo que comúnmente se denomina hardware.

- **Elementos intangibles del sistema.** Los bienes inmateriales que proporcionan las ordenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático; lo que comúnmente se denomina software.

2. Servicios informáticos. Cualquier actividad de carácter patrimonial relacionada con la actividad que desarrollan los sistemas

13 Véase más información sobre la Berkley Software Distribution (BSD) ingresando en https://goo.gl/fERhNa

informáticos y que una persona física o jurídica desarrolla a favor de otra, siendo su objeto dicho sistema.

A continuación, se revisan las principales figuras contractuales en este ámbito.

1) **Contrato de desarrollo a medida**

En este tipo de contratos, el proveedor se obliga a realizar y entregar un programa informático al contratante a cambio de un precio o una contraprestación determinada.

En estos contratos es de suma importancia:

- Fijar quién será el titular de los derechos sobre el software: el desarrollador o el cliente.
- Definir con precisión el objeto y el entorno: la documentación de los requisitos de usuarios (DRU) y la documentación de especificaciones (descripción del equipo en el que el software va a operar, sistemas operativos, otro software con los que se interconectará).
- Comprobar la solidez financiera y competencia intelectual y técnica de la empresa de software, puesto que son contratos de larga duración.
- "Fijar plazos de entrega: calendario con fases de ejecución y un sistema de comprobación de la ejecución de hitos y resolución de errores y defectos" (UNIR, s.f., https://goo.gl/poJjBh).

2) **Contrato de *escrow***

En este tipo de contratos, el desarrollador deposita el código fuente ante una tercera parte de confianza. El licenciatario podrá recuperarlo en caso de:

- desaparición (quiebra, suspensión de pagos, concurso de acreedores, disolución o liquidación);
- incumplimiento de la obligación de mantenimiento.

Se deposita ante una tercera parte de confianza un soporte informático (2 copias) con el código, manuales y documentación que no haya sido brindada con el contrato de cesión de uso, y se debe establecer el grado de obligatoriedad de las actualizaciones en relación a futuras versiones del programa.

Este tipo de contratos son actualmente muy utilizados en esquemas de teletrabajo y en modelos *freelance*.

3) Contrato de mantenimiento

Se trata de contratos mediante los cuales se pacta un servicio para asegurar la perfecta utilización y funcionamiento del software adquirido (mantenimiento correctivo), para realizar las adaptaciones que sean precisas (mantenimiento adaptativo) e introducir mejoras (mantenimiento perfectivo).

Deben incluir las formas de actuar en caso de incidentes:

- Desarrollador: debe contar con una hot line como primer punto de entrada y definir los tiempos de respuesta y las actuaciones (atención remota, desplazamiento al domicilio), dependiendo de la urgencia y gravedad del incidente.

- Cliente: debe facilitar el acceso al local, al hardware, al software y la documentación. Debe utilizar el producto conforme a las especificaciones de uso y seguir las instrucciones que le pudiera dar el desarrollador, además de consultarle cualquier modificación que pudiera repercutir en el mantenimiento.

4) Contrato SLA

También denominado contrato o acuerdo de nivel de servicio de contratación. Es un contrato mediante el cual se especifican los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo. Los niveles se miden conforme a parámetros concretos tales como:

- el tipo de servicio;
- el soporte a clientes y la asistencia (tiempo de respuesta a incidencias);
- las provisiones para seguridad y datos;
- las garantías del sistema y los tiempos de respuesta;
- la disponibilidad del sistema;
- la conectividad;
- las multas o penalizaciones por la caída del sistema (Miebach Logística, 2004).

5) **Contrato de *hosting***

Se trata de un contrato mediante el cual una persona física o jurídica (por lo general, una empresa) almacena, gestiona y realiza el mantenimiento de los archivos y sitio web de otra, que le abona una cantidad de dinero de forma periódica. Esto permite externalizar la estructura en TI (Tecnologías de Información), evitando riesgos técnicos y sustituyendo una cuota mensual por una elevada inversión en activos (servidores, líneas dedicadas).

Los contratos de hosting pueden clasificarse en dos grandes grupos tomando como criterio el contenido de la prestación:

- *Virtual* hosting o hosting en servidor compartido: la empresa de hosting (*web host*) proporciona la infraestructura TI, para lo cual paga la empresa alojada una cantidad de dinero (cuota), normalmente con carácter mensual. Puede darse el caso de que la empresa alojada requiera la exclusividad de un servidor; en este caso, la modalidad es la de servidor dedicado.

- *Housing (co-located hosting):* "la infraestructura física de TI es propiedad de la empresa alojada teniendo libertad absoluta para su gestión, en este caso el web host proporciona un espacio físico y el correspondiente ancho de banda pactado" (UNIR, s.f., https://goo.gl/poJjBh).

Contratos electrónicos

Los contratos electrónicos son aquellos realizados mediante medios electrónicos, con independencia de cuál sea su objeto; por lo tanto, son el cauce jurídico mediante el que se instrumenta la actividad económica en un sector cada vez más relevante: el comercio electrónico.

El estudio de la contratación electrónica debe partir, a su vez, del estudio de la normativa sobre comercio electrónico.

> El objetivo fundamental al que está orientada la regulación del comercio electrónico es dotar de seguridad jurídica a una actividad que, por materializarse de forma virtual sin sincronicidad física, presenta numerosos riesgos para las partes, esencialmente para el cliente o consumidor. " (UNIR, s.f., https://goo.gl/poJjBh).

En Argentina no existe aún una ley específica sobre comercio electrónico, pero se reúnen distintos elementos jurídicos para abordar la materia, los que se resumen a continuación.

Bitcoins y monedas virtuales

> RESOLUCIÓN 300/2014 de la Unidad de Información Financiera (UIF), sobre prevención del lavado de activos y de la financiación del terrorismo sugiriendo prestar atención al riesgo que implican las operaciones efectuadas con Monedas Virtuales (ej. Bitcoins), que son la representación digital de valor que puede ser objeto de comercio digital pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. (Cuervo Álvarez, s. f. a, https://goo.gl/X6jJKF).

Compras a proveedores del exterior

- Resolución General N.º 3579 de la Administración Federal de Ingresos Públicos (AFIP), que establece que los que "realicen compras de mercaderías a proveedores del exterior, que ingresen al país... [deberán completar] el Formulario Nº 4550 (Compras a Proveedores del Exterior)... con anterioridad al retiro o recepción de la mercadería"[14].

- Resolución General N.º 3582 de la Administración Federal de Ingresos Públicos (AFIP), que establece que los que

> realicen compras de mercaderías a proveedores del exterior... podrán utilizar el procedimiento previsto en la Resolución General N° 3.579 en DOS (2) oportunidades en el año calendario, resultando de aplicación la franquicia anual de VEINTICINCO DÓLARES prevista en el Artículo 80, Apartado 1, Inciso c) del Decreto N° 1001/82 [Código Aduanero] y sus modificaciones.[15]

Formulario QR de Data Fiscal

- Resolución General N.º 3377 de la Administración Federal de Ingresos Públicos (AFIP), que establece que los

14 Art. 1.º, Resolución General N.º 3579. (2014). Compras a proveedores del exterior. Administración Federal de Ingresos Públicos (AFIP). Recuperada de https://goo.gl/S2x7p4
15 Art. 1.º, Resolución General N.º 3582. (2014). Operaciones comerciales minoristas. Administración Federal de Ingresos Públicos (AFIP). Recuperada de https://goo.gl/3bUU3U

contribuyentes que vendan bienes o presten servicios a consumidores finales “deberán exhibir el Formulario Nº 960/NM - ‘Data Fiscal’, en sus locales de venta, locación o prestación de servicios..., salas de espera, oficinas o áreas de recepción”[16]. Además, la norma señala que “los sitios web... deberán colocar en un lugar visible de su página principal, el logo “Formulario Nº 960/NM “Data Fiscal”, con su correspondiente hipervínculo que esta Administración Federal proveerá a tal efecto”[17].

Contrataciones Públicas Electrónicas

- Decreto N.º 1023/2001, sobre el Régimen de Contrataciones de la Administración Pública Nacional, que establece, en Capítulo II, las Contrataciones Públicas Electrónicas[18].

Documentación electrónica en la actividad aseguradora

- Resolución N.º 33.463/08 de la Superintendencia de Seguros de la Nación, que incorpora al Reglamento de la Actividad Aseguradora “la entrega de documentación por medios electrónicos”[19].

Informes de Progreso del Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior (1999)

- Resolución N.º 412/99 del Ministerio de Economía, Obras y Servicios Públicos, que aprueba el Primer Informe de Progreso del Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior[20].

---

16 Art. 24, Resolución General N.º 3377. (2012). PROCEDIMIENTO. Régimen de emisión de comprobantes. Exhibición del Formulario Nº 960/ NM - "Data Fiscal". Resoluciones Generales Nº 1415, Nº 2676 y Nº 2746, sus respectivas modificatorias y complementarias. Norma modificatoria y complementaria. Administración Federal de Ingresos Públicos (AFIP). Recuperada de https://goo.gl/FPASDH

17 Art. 25, Resolución General N.º 3377. (2012). PROCEDIMIENTO. Régimen de emisión de comprobantes. Exhibición del Formulario Nº 960/ NM - "Data Fiscal". Resoluciones Generales Nº 1415, Nº 2676 y Nº 2746, sus respectivas modificatorias y complementarias. Norma modificatoria y complementaria. Administración Federal de Ingresos Públicos (AFIP). Recuperada de https://goo.gl/FPASDH

18 Decreto N.º 1023. (2001). Administración Pública Nacional. Contrataciones del estado – Régimen. Poder Ejecutivo Nacional. Recuperado de https://goo.gl/t2WW22

19 Resolución N.º 33.463. (2008). Modificación del Reglamento de la Actividad Aseguradora, en lo pertinente al "Contenido de Pólizas". Superintendencia de Seguros de la Nación. Recuperado de https://goo.gl/jvujPc

20 Resolución N.º 412. (1999). [Aprueba las recomendaciones formuladas por el Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior]. Ministerio de Economía y Obras y Servicios Públicos. Recuperado de https://goo.gl/vxzdSa

- Resolución N.º 1248/99 del Ministerio de Economía, Obras y Servicios Públicos, que aprueba un Segundo Primer Informe de Progreso del Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior[21].

Juegos de azar y apuestas online

Resolución General 3510/2013, de 1 de julio de 2013, de la Administración Federal de Ingresos Públicos (AFIP), que establece el Registro de Operadores de Juegos de Azar y un régimen de información respecto de la explotación de juegos de azar y/o apuestas cuya instrumentación o perfeccionamiento se realice en Argentina. Incluye a los juegos por Internet y por telefonía fija o móvil.

Resolución General 3528/2013, de 4 de septiembre de 2013, de la Administración Federal de Ingresos Públicos (AFIP), que suspende la entrada en vigencia del cronograma del art. 18 de la Resolución General 3510 hasta tanto se complete el desarrollo de los sistemas informáticos y aplicaciones tecnológicas que permitan la operatividad del régimen. (Cuervo Álvarez, s. f. b, https://goo.gl/1RFmPA).

Protección de datos personales

Los datos personales, por separado, puede que no brinden mucha información o no sean de gran utilidad, pero convenientemente tratados pueden proporcionar un perfil claro de una persona. Esto, para las organizaciones, puede significar grandes beneficios y un ahorro de costos, ya que permite ofrecer servicios más concretos y directos a sus clientes, consumidores o usuarios.

Para dar respuesta a estos perjuicios y proteger la intimidad de las personas físicas, se han establecido diferentes normativas tanto a nivel nacional como internacional.

En Argentina, la protección de datos personales se encuentra reglamentada por la Ley N.° 25.326 de Protección de Datos Personales[22], más conocida como ley de *hábeas data*. Esta establece como órgano de control a la

21 Resolución N.º 1248. (1999). [Aprueba el Segundo Informe de Progreso del Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior]. Ministerio de Economía y Obras y Servicios Públicos. Recuperado de https://goo.gl/z41zQS

22 Ley 25.326. (2000). Protección de Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O

Dirección Nacional de Protección de Datos Personales[23], dependiente del Ministerio de Justicia y Derechos Humanos de la Nación[24].

En el año 2003, la Unión Europea otorgó a la Argentina la adecuación en los términos de su Directiva 95/46/CE[25] que, entre otras facilidades, establece que al país no se le aplican las restricciones para la transferencia de datos personales, lo que permite el libre flujo de estos desde la Unión Europea. Esta adecuación es de revisión permanente y cualquier modificación a la ley es evaluada para determinar su vigencia o interrupción.

La ya mencionada Ley de Protección de Datos Personales tiene por objeto:

> la **protección integral** de los datos personales asentados en **archivos**, **registros**, **bancos de datos**, u otros **medios técnicos de tratamiento de datos**, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.[26]

Para ello, confiere una serie de derechos al titular de los datos, por un lado, y, por el otro, una serie de exigencias a los usuarios y responsables de bancos de datos de cuya información contenga datos de carácter personal.

Derechos de los titulares de los datos

La ley confiere los siguientes derechos a los titulares de los datos:

- derecho de información sobre los datos;
- derecho de acceso a los datos;
- derecho de rectificación, actualización o supresión de los datos;
- gratuidad en relación al derecho anterior[27].

[23] Véase más información sobre la Dirección Nacional de Protección de Datos Personales ingresando en http://www.jus.gob.ar/datos-personales.aspx
[24] Véase más información sobre el Ministerio de Justicia y Derechos Humanos de la Nación Argentina ingresando en http://www.jus.gob.ar
[25] Directiva 95/46/CE. (1995). Protección de los Datos Personales. Parlamento Europeo y del Consejo, Comunidad Europea. Recuperado de https://goo.gl/x5RT1T
[26] Art. 1, Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O
[27] Arts. 13-20, Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O

Sujetos que deben cumplir la ley

Los sujetos alcanzados por la ley están definidos en su Capítulo IV como *los usuarios y responsables de archivos, registros y bancos de datos*, y el artículo 26 establece que "todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control"[28].

Los bancos de datos contemplados son tipificados de la siguiente manera:

- archivos, registros o bancos de datos públicos;
- archivos, registros o bancos de datos privados;
- prestación de servicios informatizados de datos personales;
- prestación de servicios de información crediticia;
- archivos, registros o bancos de datos con fines de publicidad;
- archivos, registros o bancos de datos relativos a encuestas[29].

Los responsables de los bancos de datos deberán someter el banco de datos a un proceso de inscripción ante la Dirección Nacional de Protección de datos Personales[30]. En dicho proceso, deberán comunicar:

a) nombre y domicilio del responsable;
b) características y finalidad del archivo;
c) naturaleza de los datos personales contenidos en cada archivo;
d) forma de recolección y actualización de datos;
e) destino de los datos y personas físicas o de existencia ideal a los que pueden ser transmitidos;
f) modo de interrelacionar la información registrada;
g) medios utilizados para garantizar la seguridad de los datos. Se debe detallar la categoría de personas con acceso al tratamiento de la información;
h) tiempo de conservación de los datos;

[28] Art. 26, Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O
[29] Arts. 21-28, Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O
[30] Arts. 21-28, Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O

i) forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos que se deben realizar para la rectificación o actualización de los datos.[31]

Sanciones

La ley establece dos tipos de sanciones para los responsables de bancos de datos y usuarios:

- Sanciones administrativas:
  - "apercibimiento,
  - suspensión,
  - multa de mil pesos ($ 1000.-) a cien mil pesos ($ 100.000),
  - clausura o cancelación del archivo, registro o banco de datos"[32].

- Sanciones penales:

  - prisión de 1 mes a 2 años en casos de inserción de datos falsos;
  - prisión de 6 meses a tres años en casos de difusión de información falsa;
  - prisión de 1 mes a dos años ante casos de acceso no autorizado;
  - prisión de 1 mes a dos años ante revelación no autorizada;
  - cuando el responsable sea un funcionario público, aplica además la inhabilitación para el desempeño en cargos públicos[33].

Por último, el órgano de control, en la figura de la Dirección Nacional de Protección de Datos Personales, es el responsable de atender las denuncias y reclamos efectuados, y será quien investigue si la base de datos denunciada da cumplimiento o no a los principios que establece la ley y las disposiciones reglamentarias.

Peritaje informático

El peritaje informático, o informática forense, se ubica dentro de las ciencias forenses, en el marco de las ciencias criminalísticas, como ámbito

[31] Art. 21, Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O
[32] Art. 31, Ley 25.326. Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O
[33] Art. 32, Ley 25.326. Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/AgjI1O

especializado en el tratamiento de pruebas o evidencias relacionadas con las tecnologías de la información y las comunicaciones.

Puede definirse como "el proceso de identificar, preservar, analizar y presentar evidencia digital de manera que esta sea legalmente aceptable" (Herrera y Gómez, 2009, diap. 3). Surge como una disciplina auxiliar de la justicia moderna para proveer conocimientos, técnica y garantías sobre de la verdad alrededor de la evidencia digital, útil en un proceso judicial.

Evidencias digitales

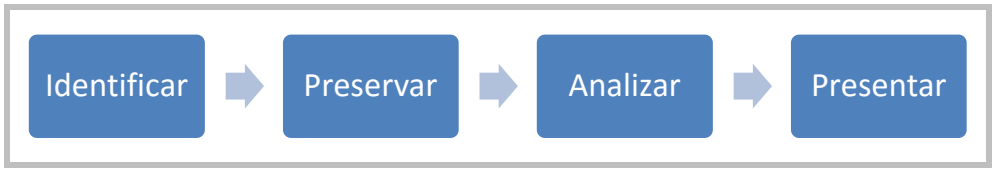
Los medios de prueba informática se basan en la utilización de evidencia digital sobre la que se aplican técnicas de informática forense.

La evidencia o prueba digital reúne características muy particulares que la distinguen de cualquier otra prueba material: es volátil y susceptible de ser alterada.

En el ámbito judicial, es de vital relevancia que la investigación sobre medios informáticos sea efectuada a través de un proceso metodológico que posibilite la repetición de todos sus pasos ante un tribunal, cuando sea necesario.

En la actualidad, existen varias metodologías de trabajo para la realización de análisis de evidencias, aunque en su mayoría adoptan el modelo presentado en la siguiente figura.

Figura 1: Proceso de análisis de evidencia en peritaje informático



Fuente: adaptación propia con base en Gómez, 2004.

En donde:

- **Identificación:** es la identificación del entorno, medio o dispositivo que puede contener evidencia.
- **Preservación:** es la preservación del entorno, medio o dispositivo objeto de evidencia digital contra daños accidentales o intencionales que se puedan producir desde su identificación hasta la correspondiente

presentación. La necesidad de preservación de la evidencia digital abarca todo el proceso de trabajo.

- **Análisis:** es el análisis al que se somete al entorno, medio o dispositivo en busca de evidencia o información útil.
- **Presentación:** es la exposición de los hallazgos obtenidos a través de un informe pericial ante las partes interesadas.

Vale la pena mencionar el estándar ISO/IEC 27037:2012, denominado Tecnologías de Información. Técnicas de Seguridad. Guía para identificación, recolección y adquisición y preservación de evidencias digitales[34]. Es un estándar que vino a cubrir una falta de estandarización en la materia. Su adopción no es inmediata debido a que, para ello, se deben adecuar las reglamentaciones locales.

Cadena de custodia

La cadena de custodia aplica al segundo paso de la metodología de análisis de evidencia, y atraviesa todo el proceso.

Para que la evidencia digital sea considerada como válida y adquiera valor probatorio ante la Justicia, es necesario garantizar confiabilidad; esto implica evitar suplantaciones, modificaciones, alteraciones, adulteraciones o su destrucción total, hecho que ocurre con frecuencia con las evidencias digitales, ya sea mediante borrado o denegación de servicio.

Desde la recolección hasta la disposición final, debe implementarse un procedimiento con soporte teórico científico, metodológico criminalístico, estrictamente técnico y procesalmente adecuado. Si el procedimiento carece de cualquiera de estos componentes, la evidencia digital recolectada no alcanzará el valor probatorio pretendido.

Este procedimiento se caracteriza por involucrar a múltiples actores, quienes deben tener profundamente claro el rol que deben cumplir dentro de este, las actividades que deben desarrollar durante la manipulación de la prueba y sus responsabilidades derivadas.

La cadena de custodia informático-forense se puede definir como:

[34] Véase más información acerca del ISO/IEC Standard No. 27037 (2012), denominado *Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence,* en la web de la International Organization for Standardization & International Electrotechnical Commission, disponible en https://www.iso.org/standard/44381.html

> un procedimiento controlado y supervisable, que se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene como fin asegurar la confiabilidad de la evidencia digital recolectada en un determinado lugar del hecho real o virtual desde su recolección hasta su disposición definitiva por orden judicial. (Darahuge y Arellano González, 2012).

En la bibliografía básica[35], se abordan distintas herramientas utilizadas en el ámbito del peritaje informático.

En resumen, y a modo de conclusión, es importante tener en cuenta las siguientes cuestiones:

- el software se asimila a una obra literaria, artística o científica; es considerado propiedad intelectual y está protegido por derechos de autor. La concesión de estos derechos a terceras partes, sea para uso o explotación se materializa a través de distintos modelos de licencia.

- En materia de contratos informáticos, o de servicios informáticos, se han revisado los modelos más relevantes y utilizados en el mercado. La contratación electrónica es uno de los pilares del comercio electrónico, cuya regulación pretende proteger a las partes que intervienen, en mayor medida al cliente o consumidor, y dicha protección estará siempre sujeta a la jurisdicción a la que ambas partes acuerden someterse para resolver los conflictos eventuales que puedan surgir durante una transacción.

- La protección de datos personales, si bien se trata de una temática jurídica, tiene implicancias directas en la seguridad de la información de la organización y, por lo tanto, debe ser contemplada desde las fases iniciales de un diseño de política de seguridad.

- En un contexto de análisis y gestión de riesgos, descuidar los aspectos legales y regulatorios sugiere un riesgo jurídico, con lo cual requiere un tratamiento para minimizarlo.

- Con respecto al peritaje informático, su lado más sensible tiene que ver con el tratamiento de las evidencias digitales, dada la particularidad que estas revisten. Su volatilidad, facilidad de reproducción y la incapacidad para distinguir una copia de su original exigen un tratamiento metodológico que asegure su validez probatoria para certificar con ello todo el proceso de la cadena de custodia.

[35] Véase el *Manual de Informática Forense II,* de Darahuge y Arellano González (2012).

Referencias

Barbosa Ruiz, A. J., y Alfaro Arriola, R. (2013). *El uso del software libre a la luz de la ley de derechos de autor* [Tesis de Pregrado]. Universidad Centroamericana, Nicaragua. Recuperada de http://repositorio.uca.edu.ni/1783/1/UCANI3518.PDF

Constitución Nacional Argentina. (1994). [Aprobada por Ley 24.430]. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/6tYK6J

Cuervo Álvarez, J. (s. f. a). Legislación Informática de Argentina 2014. *Revista Informática Jurídica*. Recuperado de http://www.informatica-juridica.com/legislacion/argentina/y2014/

Cuervo Álvarez, J. (s. f. b). Legislación Informática de Argentina 2013. *Revista Informática Jurídica*. Recuperado de http://www.informatica-juridica.com/legislacion/argentina/y2013/

Darahuge, M., y Arellano González, L. (2012). *Manual de Informática Forense II*. Buenos Aires, AR: Errepar.

Decreto N.º 1023. (2001). Administración Pública Nacional. Contrataciones del estado – Régimen. Poder Ejecutivo Nacional. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/65000-69999/68396/texact.htm

Directiva 95/46/CE. (1995). Protección de los Datos Personales. Parlamento Europeo y del Consejo, Comunidad Europea. Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l14012

Gómez, L. (2004). El tratamiento de la evidencia digital. Recuperado de https://drive.google.com/file/d/0B5NohtWrhSPaRWxMRFdLd2ZuaGc/edit

Herrera, H., y Gómez, S. (2009). *Informática forense* [PPT en línea]. Recuperado de http://www.neuquen.gov.ar/seguridadinformatica/pdf/Informatica%20Forense%20-%20Hernan%20Herrera.pdf

Ley 11.723. (1933). Régimen Legal de Propiedad Intelectual. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/VNFmHa

Ley 25.036. (1998). Propiedad Intelectual [Modificatoria de la Ley 11.723, Régimen Legal de la Propiedad Intelectual]. Honorable Congreso de la Nación Argentina. Recuperado de https://goo.gl/6Vo2Yx

Ley 25.326. (2000). Protección de los Datos Personales. Honorable Congreso de la Nación Argentina. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

Miebach Logística. (Septiembre y octubre de 2004). *SLA en Logística. Definición y Elementos del SLA® en el entorno logístico*. Seminario IIR, Barcelona y Madrid. Recuperado de http://chiletransporte.cl/portal/images/Documentos/AcuerdosNivelDeServicioEnLogisticaYTransporte.pdf

Resolución General N.º 3377. (2012). PROCEDIMIENTO. Régimen de emisión de comprobantes. Exhibición del Formulario Nº 960/ NM - "Data Fiscal". Resoluciones Generales Nº 1415, Nº 2676 y Nº 2746, sus respectivas modificatorias y complementarias. Norma modificatoria y complementaria. Administración Federal de Ingresos Públicos (AFIP). Recuperada de http://biblioteca.afip.gob.ar/dcp/REAG01003377_2012_08_28

Resolución General N.º 3579. (2014). Compras a proveedores del exterior. Administración Federal de Ingresos Públicos (AFIP). Recuperada de http://www.informaticalegal.com.ar/2014/01/20/resolucion-general-3579-administracion-federal-de-ingresos-publicos-afip-compras-a-proveedores-del-exterior/

Resolución General N.º 3582. (2014). Operaciones comerciales minoristas. Administración Federal de Ingresos Públicos (AFIP). Recuperada de http://biblioteca.afip.gob.ar/dcp/REAG01003582_2014_01_21

Resolución N.º 412. (1999). [Aprueba las recomendaciones formuladas por el Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior]. Ministerio de Economía y Obras y Servicios Públicos. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/55000-59999/56911/norma.htm

Resolución N.º 1248. (1999). [Aprueba el Segundo Informe de Progreso del Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior]. Ministerio de Economía y Obras y Servicios Públicos. Recuperado de http://www.informaticalegal.com.ar/1999/10/19/resolucion-n-124899-ministerio-de-economia-obras-y-servicios-publicos-segundo-informe-de-progreso-del-grupo-de-trabajo-sobre-comercio-electronico-y-comercio-exterior/

Resolución N.º 33.463. (2008). Modificación del Reglamento de la Actividad Aseguradora, en lo pertinente al "Contenido de Pólizas". Superintendencia de Seguros de la Nación. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/145000-149999/145133/norma.htm

Universidad Internacional de la Rioja (UNIR). (s. f.) *Contratación informática.* Recuperado de: https://www.scribd.com/document/288034052/Contratacion-informatica