[Curso de Hacking Ético](https://platzi.com/clases/ethical-hacking/)

**ArtículoContratos, Reglas de compromisos, Cláusula de no competencia y Acuerdo de confidencialidad**

[**Alan Joaquín Baeza Meza**](https://platzi.com/%40ajbaeza)

26 de Abril de 2019

**Definición 1:**
Los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de **contratos**, el cual para su existencia se requiere de:

* Consentimiento de las partes.
* Objeto que pueda ser materia del contrato.

**Definición 2:**
Hay que recordar que un contrato establece las **bases de trabajo, disponibilidad y entregas** que tenemos entre las organizaciones y los proveedores de servicios.

**¿Qué son los contratos informáticos?**
Permiten transmitir derechos de propiedad o de uso sobre bienes como equipos (hardware) o programas (software) y sobre todo los referentes a la prestación de servicios sobre este tipo de bienes.

**Los contratos informáticos pueden dividirse en múltiples categorías, como:**
-**Contratos relativos al hardware:** Se establecen los elementos físicos de un equipo electrónico y la modalidad en las cuales se van a adquirir (compra/venta o arrendamiento).

* **Contratos de licencia de software:** Son aquellos en los cuales una persona u organización tiene los derechos sobre un software como autor y concede a un licenciatario la autorización de poder utilizarlo.
* **Contratos de desarrollo de una página web:** En este contrato se especifica por el cual una persona solicita a otra el diseño, desarrollo y mantenimiento de un sitio web.
* **Contratos de mantenimiento:** Es aquel que busca que tanto el hardware como el software de manera individual o conjunta, se mantengan en las condiciones óptimas para poder seguir operando, evitando la existencia de fallos o bien resolver aquellos errores que ya están presentes en el funcionamiento de los equipos electrónicos.

**Contratos para realizar un Pentesting**
Es aquel que tiene como objeto permitir a un agente externo especializado realizar una serie de análisis durante un periodo cierto con el propósito de evaluar el cumplimiento de los derechos y obligaciones contraídos al haber comprado o arrendado algún software y/o hardware.
Este tipo de contratos deben incluir todas las cláusulas necesarias, así como establecer los derechos y responsabilidades de las partes involucradas en el proceso.
Una recomendación es que el contrato sea redactado por un abogado, pero debe estar firmado por la persona que realizar la prueba pertinente y sobre todo la organización. Por lo general un contrato bien elaborado debe considerar estos puntos:

* **Cláusula de no divulgación:** La organización redacta esta cláusula para salvaguardar su información confidencial.
* **Objetivos del Pentesting:** En esta sección del contrato se establecen las razones para realizar la prueba de penetración, los objetivos y el alcance de la prueba.
* **Cuotas y calendario de proyectos:** Se establecen las opciones de pago y precios del servicio Pentesting, así como el calendario de actividades a realizar.
* **Información sensible:** En este apartado se incluye información relacionada con los activos de la organización, el desarrollo de aplicaciones, los parámetros de seguridad de la red u otra información confidencial que requiera el equipo que realizara las pruebas.
* **Información confidencial:** Esta información incluye secretos comerciales, red, sistema telefónico, datos del cliente, materiales comerciales. Esta información se proporciona al prestador del servicio de manera confidencial, con la condición de esta no se divulgue a una tercera persona, compañía, a menos que se mencione en la autorización por escrito de la parte que confía.
* **Cláusula de indemnización:** Mediante esta cláusula se protege al prestador del servicio de cualquier problema legal o financiero, en caso de que el Pentesting resulte en una pérdida o daños a los activos de la organización.
* **Informes y responsabilidades:** Las pautas del contrato establecen la metodología para permitir los procedimientos de prueba e informe y el período de tiempo para la tarea asignada.

**Reglas de compromiso:**
Las reglas de compromiso por sus siglas en ingles ROE (Rules of engagement) es el permiso formal para realizar un Pentesting. Proporcionan ciertos derechos y restricciones al equipo de pentesting para realizar la prueba, y ayudan a los evaluadores a superar las restricciones legales, federales y relacionadas con las políticas para utilizar diferentes herramientas y técnicas de pruebas de penetración.

¿Qué debe contener un ROE?

* Establecer el contacto por parte del equipo de pentesting, la organización y otros involucrados como administradores de sistemas o red.
* Direcciones IP/rangos que serán analizados.
* Redes y equipos que estarán restringidos.
* Una lista de las técnicas (DoS, Ingeniería social) y herramientas permitidas (Sniffers).
* Fecha y hora en que se realizará la prueba.
* Identificar el periodo de duración y culminación de la prueba.
* La dirección IP del equipo que utilizará el pentester, para diferenciar los ataques de prueba a uno real.

**Acuerdo de confidencialidad y de no divulgación:**
Estos documentos son importantes contar con ellos antes de comenzar un Pentesting, en el acuerdo de confidencialidad se establece que la información que proporciona la organización es confidencial y propietaria. Este acuerdo también cubre aspectos clave en caso de negligencia y responsabilidad para muchos problemas potenciales, es importante conocer si la empresa cuenta un seguro por daños.

Un acuerdo de confidencialidad (NDA, por sus siglas en inglés) protege la información confidencial de una organización, recomienda que se realice escrita ya que es una herramienta legal poderosa, que establece que ninguna parte divulgará secretos comerciales, patentes u otra información propietaria a nadie fuera de la compañía. Cualquiera de las partes puede iniciar una acción legal si se incumple este acuerdo documentado.
Por aspectos ética ambas partes tienen la responsabilidad de proteger las herramientas, técnicas, vulnerabilidades e información de la divulgación más allá de los términos especificados en un acuerdo por escrito.

Algunos de los puntos a considerar son:

* Identifica la información sensible y crítica de la organización.
* Hay que especificar claramente que las partes no deben revelar información que se mencionan en el acuerdo.
* Identificar claramente todas las partes involucradas en el acuerdo.
* Incluir la fecha de inicia y cuál será la duración del periodo de no divulgación.

*Cláusula de no competencia:*\*
Si la compañía que nos contrata solicita que no se brinde el mismo servicio a su competencia, se hará uso de esta cláusula, en la cual debe quedar claramente quienes son los competidores directos y el tiempo que se aplicarán estas restricciones.

Más información: <https://drive.google.com/open?id=18WYgv-R3zM_r5eeq_9NBo1wMYPe5MjwK>