Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: IX Número: Edición Especial. Artículo no.:106 Período: Octubre, 2021

TÍTULO: Derecho, informática y corrupción. Un enfoque a la realidad ecuatoriana.

AUTORES:

1. Máster. Alberto Leonel Santillán Molina.
2. Máster. Nelly Valeria Vinueza Ochoa.
3. Máster. Cristian Fernando Benavides Salazar.

RESUMEN: Los sistemas informáticos están configurados específicamente de acuerdo a las necesidades institucionales; no obstante, si el administrador excede la autorización concedida por el titular ejecutando actos dolosos que alteren, manipulen o modifiquen datos informáticos, incurren en actos de corrupción sancionados por la ley; por tanto, el objetivo del trabajo consistió en explicar la importancia del fortalecimiento de las medidas de seguridad, auditoría y control de acceso a los sistemas automatizados de información, que no permitan su vulneración, y prevenir la ejecución de diferentes conductas ilícitas. Se usaron métodos como el histórico-lógico, analítico-sintético y como técnica el análisis de contenido, justificándose la necesidad del aseguramiento de los sistemas informáticos con medidas de seguridad físicas y lógicas.

PALABRAS CLAVES: seguridad en los sistemas informáticos, actos de corrupción, administrador del sistema, hackeo, delito informático.

TITLE: Law, computing, and Corruption. An approach to the Ecuadorian reality.

AUTHORS:

1. Master. Alberto Leonel Santillán Molina.
2. Master. Nelly Valeria Vinueza Ochoa.
3. Master. Cristian Fernando Benavides Salazar.

ABSTRACT: Computer systems are specifically configured according to institutional needs; However, if the administrator exceeds the authorization granted by the owner by executing malicious acts that alter, manipulate or modify computer data, they incur acts of corruption sanctioned by law; therefore, the objective of the work consisted of explaining the importance of strengthening security measures, auditing and access control to automated information systems, which do not allow their violation, and preventing the execution of different illegal behaviors. Methods such as historical-logical, analytical-synthetic, and content analysis as a technique were used, justifying the need to secure computer systems with physical and logical security measures.

KEY WORDS: Security in computer systems, acts of corruption, system administrator, hacking, computer crime.

INTRODUCCIÓN.

El desarrollo de las TICs tiene su génesis luego de la Segunda Guerra Mundial, donde las grandes potencias como Estados Unidos de Norteamérica y la Unión de Repúblicas Socialistas Soviéticas (U.R.S.S.) iniciaron una carrera armamentista por el manejo a nivel mundial de la hegemonía económica, cultural, política y militar, lo que aceleró de manera abismal el espionaje entre naciones, con la finalidad de poder obtener aquellos secretos que se manejaban tanto social, político y principalmente militar, situación que impidió una comunicación directa y rápida para evitar un holocausto nuclear, por lo que se instaló una conexión mediante un teléfono que tenía vínculo directo entre el Kremlin y la Casa Blanca.

Esta forma de espionaje mutuo fue conocida como la Guerra Fría, en la que existían enfrentamientos armados entre las dos potencias a través de las agencias de inteligencia, esto es la "KGB Komitet Gosudarstrennoaja Bezopasnosty" (Diario El Pais, 2021, pág. 2), por el lado ruso y la Agencia Central de Inteligencia CIA, por el lado norteamericano; sin embargo, se manejó un sistema de comunicación denominado ARPANET (Historia de redes informaticas, 2018, pág. 5) cuyas siglas en inglés significan: *Advance Researsch Project Agency Net"* (Aboso, 2017, pág. 5), que tenía como finalidad primordial mantener un canal de comunicación abierto entre las agencias de inteligencia y así evitar filtraciones de información que perjudicaría a ambas potencias.

Este sistema avanzado de comunicación era, para ese entonces, muy novedoso, el cual fue desarrollado con el paso de los años, tecnificando el mismo e insertando los avances tecnológicos de comunicación, a través de los espacios radio eléctricos, cableado de cobre, ondas electromagnéticas o satelital (Quiroz Martinez, et al., 2020).

Las tecnologías de la información y comunicación han permitido el desarrollo de la sociedad de una manera mucho más acelerada, al punto de que todas las actividades operativas de las empresas, negocios e instituciones públicas o privadas, se manejan de manera automática, permitiendo el acceso de usuarios a las diferentes plataformas digitales, de manera ordenada haciendo las actividades mucho más eficaces y eficientes (Vásquez, et al., 2021).

En la República del Ecuador las instituciones públicas han automatizado sus operaciones, con la finalidad de prestar un mejor servicio a la colectividad; no obstante, el manejo de los procesos operativos de estos sistemas de tratamiento de información, se encuentran activamente gerenciados por aquellos servidores públicos jerarquizados dentro del mismo ordenamiento jurídico ecuatoriano en materia administrativa, con formación técnica y profesional en informática (Falcón et al., 2021).

Todo sistema informático se encuentra construido en base a un software que está configurado para que funcione conforme a las necesidades de la institución para quien ha sido implementado, cuyo

manejo del proceso de "*hardening*" dificulta las acciones que vulnerarían las seguridades tanto informáticas como de la información, evitando así el acceso no autorizado a los sistemas automatizado de información, y posteriormente el espionaje o sabotaje informático (Abdel-Aal, et al., 2018).

El manejo de la configuración robusta de las medidas de seguridad de la información e informática o "*hardening*" son encargadas a un funcionario específico de acuerdo al perfil profesional informático que para el efecto tenga el funcionario, cuyas acciones son totalmente desconocidas para el resto de servidores que ejecutan el programa de acuerdo a las necesidades de la institución requirente, estas son las personas que manejan la programación del sistema y su funcionalidad.

Se puede sostener, que en esta relación tecnológica de configuración y ejecución de un software, al menos se tiene dos actores, uno es el funcionario que ejecuta el proceso de *hardening*, y el usuario final que ejecuta el programa configurado por la institución para que preste funcionalidad al tenor de su misión y visión.

Bajo estas circunstancias, es necesario explicar cómo se encuentra estructurado la conducta de hackeo o acceso no autorizado a los sistemas automatizados de información en el campo doctrinario. Es así, que la primera conducta se presenta cuando se accede, altera, modifica o manipula las medidas de seguridad que se encuentran establecidas para impedir el acceso sin los permisos respectivos, a través de la vulneración al sistema informático con herramientas que utiliza el atacante y que principalmente son desarrollos predefinidos para correr en sistemas operativos Linux bajo licencia *open source,* las mismas que se pueden encontrar en un sinnúmero de distribuciones que basados en la experiencia del atacante; estas herramientas le permiten buscar y encontrar vulnerabilidades que le faciliten el acceso no autorizado, creándose cuentas, y en consecuencia, elevar sus privilegios en las mismas, para ejecutar actos atentatorios al sistema informático, tales como la sustracción de información, el daño al sistema informático o simplemente obtener información confidencial para su

propio beneficio o de terceros, y la segunda conducta es cuando el agente supera los privilegios de usuario para el manejo del sistema, ejecutando actos, que a pesar de ser funcionalmente operativos, no son autorizados por el titular que mantiene permisos de administrador.

Esta alteración manipulación o modificación requiere que el "Insider hacker" o hacker interno, tenga acceso a este sistema a través de su permiso de manejo que fue debidamente dispuesto por el administrador, partiendo del punto de que el software ha sido construido con la finalidad de prestar una funcionalidad específica, en atención a la necesidad de la empresa negocio o institución que sirve a la comunidad, por lo que es aquí donde se altera, manipula o modifica la funcionalidad operativa del mismo, sin necesidad de que exista un rompimiento de las medidas de seguridad.

La falta de medidas de seguridad, auditoría y control de los sistemas automatizados de información, permiten su alteración, modificación y manipulación de datos informáticos, permitiendo así la ejecución de diferentes conductas contrarias a derecho en beneficio de terceros, perjudicando a la empresa, negocio o institución pública dueña del sistema.

Por lo tanto, el objetivo de la investigación radica en explicar la importancia del fortalecimiento de las medidas de seguridad, auditoría y control de acceso a los sistemas automatizados de información, que no permitan su alteración, modificación y manipulación de datos informáticos, y así prevenir la ejecución de diferentes conductas contrarias a derecho en beneficio de terceros.

DESARROLLO.

Métodos.

Para el desarrollo de la investigación se emplearon los siguientes métodos:

1. Histórico. Para identificar las principales líneas de la evolución de la informática y el derecho y el delito de hackeo en sus diferentes conductas, así como la corrupción desde el campo doctrinario.

2. Análisis lógico. Aplicado a la definición de los conceptos y variables fundamentales relacionadas con el tema.
3. Análisis jurídico-comparado. Aplicado a disposiciones jurídicas ecuatorianas e internacionales y hacer comparación de los elementos relacionados al Derecho, informática y corrupción.
4. Técnica de investigación científica. Se utilizó el análisis de documentos, con especial atención a la aplicación del análisis de contenido en cuanto a la informática y Derecho.

Las TICs y su relación con la Sociedad de la Información.

La sociedad de la información se la puede definir como aquel grupo social que tiene como objetivo "la captación almacenamiento y transmisión informática de información desde el campo social, cultural, económico, financista, que procura cambios socio económicos importantes" (Hilbert, 2009, pág. 27), que tiene como finalidad fundamental el "impulsar los cambios profundos en el conglomerado humano, principalmente por los medios disponibles, para crear y divulgar la información mediante tecnologías digitales" (CEPAL, 2013, pág. 27).

Esta comunidad permite de una manera globalizada determinar ciertas fuentes de interconexión telemática, que agilita los procedimientos en favor de los ciudadanos, tales como la comercialización y adquisición de cualquier producto mediante conexión en las diferentes plataformas digitales que ofrecen estos servicios en la red, así como también la obtención de bienes de consumo, transferencias de dinero, o en definitiva el tráfico de información personal a través de redes sociales como Facebook, Instagram, YouTube, WhatsApp, etc. (Busón, 2020).

Este conglomerado social se caracteriza principalmente por globalizar a nivel mundial el uso de las TICs, que se encuentran constituidas por "dispositivos tecnológicos que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información, que posibilitan la interacción personal con herramientas de intercambio, difusión, gestión y acceso al conocimiento"

(Desongles Corrales, 2006, pág. 14), que fomentan de manera generalizada el proceso enseñanza-aprendizaje informático y reducir la "brecha digital" (Programa de las Naciones Unidas para el Desarrollo, 2002, pág. 47) que existe con los países industrializados y aquellos en vías de desarrollo, y así evitar el retraso de estas sociedades y tener un libre flujo de información y conocimiento que disminuya la diferencia generacional entre estas sociedades.

Otra de las características que se puede individualizar en la sociedad de la información, es la comunicación inmediata a través de las diferentes redes sociales, que permiten una mayor influencia en las decisiones políticas, sociales, culturales, artísticas, etc., y el adelantamiento del desarrollo que en auxilio de las TICs optimizan en los campos industriales, económicos y políticos los procesos de producción manufactura y comercialización de productos que llegan generalmente al usuario final a través de esta transformación digital (Pacheco, 2009).

En esta cuarta revolución industrial se puede encontrar varios tipos de sociedades de la información, es así que "la 1.0 hace referencia aquella sociedad agraria y posteriormente industrial que prevaleció entre los siglos VIII hasta finales del siglo XX en el que generalmente se establecía el paradigma de aprender haciendo, enseñando aquellas ideas y destreza a los más jóvenes los cuales se transmitían a sus predecesores" (Cobo Romani, 2009, págs. 48-49).

La interconexión en internet así como el uso de las tecnologías de la información y comunicación, permitió el nacimiento de la sociedad 2.0 a través del uso de herramientas tales como la "Web 2.0, el uso de las redes sociales en una plataforma de intercambio de ideas e instrumentos de comunicación como por ejemplo los blogs, wikis, YouTube, que han permitido el uso masivo del internet y la aparición de nuevas labores colectivas como el periodismo ciudadano, actividades científicas e intercambio de información" (Cobo Romani, 2009, pág. 51).

Actualmente, se habla de la sociedad 3.0 que se sustenta en el acelerado y vertiginoso crecimiento exponencial tecnológico, que sostiene el postulado de que "a mayor crecimiento del orden, mayor

aceleración del tiempo" (Kurzweil, 1999, pág. 30), por la idea de que a medida de que "la tecnología avanza también lo hace la sociedad" (Morgan, 1877, pág. 26), haciendo imposible predecir el futuro con un avance tecnológico que va a pasos agigantados y de la mano con la evolución de la web 3.0 y 4.0 donde ya se está desarrollando la inteligencia artificial.

La sociedad de la información es un referente de desarrollo en todas sus clases, sea esta social, cultural, jurisdiccional que obliga al ser humano, en su meta de seguir evolucionando en esta carrera digital, a intercambiar datos para un desarrollo personal, profesional y social en uso de las Tecnologías de la Información y comunicación.

Las diferentes conductas en el delito de hackeo y la corrupción del insider hacker.

El hackeo se puede definir como el acceso no autorizado a los sistemas automatizados de información, mediante la vulneración de las medidas de seguridad impuestas por el titular del sistema, ampliándose dicha definición desde el punto de vista doctrinario, para aquellos actos realizados por el que tiene los permisos de administrador, el cual excede la autorización que le ha sido otorgado por el titular, realizando actos de alteración, manipulación o modificación de datos informáticos, permitiendo que el sistema realice una acción distinta por la que fue configurada para que preste su funcionalidad, esto en atención a la necesidad institucional y apegada a las normas legales.

Existen metodologías que se realizan con la finalidad de explotar todas las vulnerabilidades que presenta un sistema automatizado de información, para permitir el acceso al mismo con el objetivo de fortalecer las mismas, tratándose del hacking ético, estableciendo cuáles son los puntos de penetración y de mayor riesgo de intromisión, y de esta manera, en una auditoría, presentar un informe al titular para que tome las medidas de seguridad informática y de la información acorde a sus necesidades.

El hacker oscuro realiza las mismas metodologías, solo que su objetivo es diferente, ya que busca acceder sin permiso a dicho sistema, con el propósito de realizar un espionaje informático, sabotaje informático u obtener un beneficio material o inmaterial propio o para un tercero.

Los procedimientos que se utilizan para poder llegar a determinar esta clase de actos desde la informática, se les denomina: "test de penetración; el test de vulnerabilidad y el *pentesting*" (González Pérez, 2015, págs. 66-68).

El test de penetración consiste en realizar pruebas ofensivas contra los mecanismos de defensa que existen dentro del entorno que analizará el hacker, con la finalidad de establecer cuáles son los puntos donde se puede realizar este acceso indebido. El test de vulnerabilidad realiza el análisis de las vulnerabilidades que presenta el sistema, y así establecer una priorización de cuál es el riesgo que exterioriza cada uno de estos accesos, y presentar de manera clara y precisa cuáles son los puntos más vulnerables del sistema que puedan ser de fácil acceso para una penetración; y finalmente el *pentesting* es un ataque al sistema automatizado de información con el objetivo de encontrar las debilidades en las seguridades del sistema, que permita el acceso o la alteración, manipulación o modificación de la funcionalidad del sistema operativo o datos informáticos que constan en el mismo.

Las medidas de seguridad que se utilizan sirven para garantizar en el sistema la confidencialidad integridad y disponibilidad de datos, tales como: "reconocimiento de patrones de voz, lector del iris del ojo, reconocimiento biométrico facial, huella dactilar, y el usuario y contraseña que permite el acceso al sistema operativo" (Suarez, 2016, pág. 344).

Se pueden identificar tres clases de hacker, así el hacker ético, el hacker oscuro y el *insider hacker*. El hacker ético se lo puede definir como aquella persona que realiza "la aplicación de metodologías específicas con herramientas como inteligencia artificial, para realizar una serie de pruebas que permitan identificar todas las vulnerabilidades posibles, y con esta auditoría de seguridad y la

implementación de medidas que contrarresten la intromisión, garantizarían el impedir el acceso al sistema" (Ardila, Salcedo, Pedraza, & Saavedra, 2020, pág. 12).

Las fases que son usada como metodologías para realizar los test de penetración o el *pentesting*, y que son utilizados tanto por el hacker ético como el hacker oscuro son: "1. Fase de reconocimiento; 2. Fase de exploración; 3. Fase de obtención de acceso; 4. Fase de mantenimiento del acceso; y 5. Fase cubrimiento de huellas" (González, 2019, pág. 13).

La fase de reconocimiento o *footprint* es aquella que realiza el hacker con la finalidad de identificar plenamente cuál es el sistema que va a hackear, con la finalidad de identificar las vulnerabilidades y pasar a la fase de exploración, que es aquella en la que se realiza el análisis de las vulnerabilidades que presenta el sistema, y allí proceder posteriormente a la obtención del acceso.

Este acceso se realiza a través de la vulneración al sistema informático con herramientas que utiliza el atacante, y que principalmente, son desarrollos predefinidos para correr en sistemas operativos Linux bajo licencia *open source*, las mismas que se pueden encontrar en un sinnúmero de distribuciones, que basados en la experiencia del atacante, estas herramientas le permiten buscar y encontrar vulnerabilidades que le faciliten el acceso no autorizado, creándose cuentas, y en consecuencia, elevar sus privilegios en las mismas, para ejecutar actos atentatorios al sistema informático, ya en la fase de mantenimiento del acceso, tales como la sustracción de información, el daño al sistema informático o simplemente obtener información confidencial para su propio beneficio o de terceros, para finalmente, realizar el borrado de huellas y así evitar identificar al hacker que realizó el ataque.

Una de las particularidades que presenta el manejo de los sistemas automatizados de información, son los permisos de administrador que son entregados a aquella persona que maneja el sistema, tanto en su operatividad como en la funcionalidad del mismo, los que son entregados con el objetivo de que puedan manejarlo en cuanto a la funcionalidad de este.

Es aquí, donde se presenta el exceso en la autorización dada por el titular, cuando la persona tiene permiso tan sólo para poder acceder a cierta parte del sistema operativo superando la autorización conferida este, y de esta manera, alterando, manipulando o modificando la funcionalidad del sistema para su beneficio o de un tercero. A esta persona se lo conoce como *insider hacker*, a quién se le define como aquel que se encuentra en el interior de la empresa, negocio o institución del sector público, y que realice esta clase de actos indebidos e ilegales para beneficiarse material o inmaterialmente, o para los mismos beneficios en favor de un tercero.

En la actualidad, se puede identificar que no solamente la conducta de hackeo aborda la vulneración de las medidas de seguridad de los sistemas automatizados de información, a través de las herramientas que para el efecto han sido construidas, e identificar las vulnerabilidades para explotarlas, sino también, cuando se excede en la autorización dada por el titular para poder acceder a ese sistema, realizando actos para los cuales no ha tenido el permiso respectivo, y de esta manera, alterar, modificar o manipular los datos informáticos para que ejecute una tarea que no ha sido programada.

El proceso de *Hardening* y del administrador del sistema.

El proceso de *hardening* (Gómez, 2014, pág. 52) también llamado “endurecimiento de la seguridad informática, consiste en el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo. Esto se logra eliminando software; servicios, usuarios, accesos innecesarios, cerrando puertos que no están en uso” (Centro de innovación y soluciones empresariales y tecnológicas, 2020, pág. 5).

Las alternativas que se presentan para poder asegurar este proceso de endurecimiento informático, que impida el hackeo a los sistemas automatizados de información son:

a) Cambiar todas las claves de acceso que para el efecto tenga el sistema y que vengan por defecto, como por ejemplo el puerto 8080 que se encuentra habilitado por defecto para el acceso al internet.
b) La desinstalación de todo software que no sea necesario para la operatividad del sistema o que definitivamente haya venido preinstalado y que pueda servir como punto de acceso para una penetración mediante un ataque informático.
c) Revisar todos los usuarios que se encuentran en el sistema y deshabilitar el acceso que no presenten necesidad dentro de la funcionalidad del mismo y que no tenga ninguna relación con el sistema a cuidar.
d) Deshabilitar todos aquellos servicios que no presten ninguna garantía de seguridad de la información o que no se estén utilizando, y que definitivamente puedan ser considerado como un punto vulnerable de acceso.
e) De los 65536 puertos lógicos que tiene todo sistema, deben cerrarse aquellos que no se encuentren en uso.
f) Instalar firewall o corta fuegos.
g) Utilizar copias de seguridad como respaldo para la información importante y sensible.
h) La actualización de software que permitan instalar los parches de seguridad que impidan el acceso por el lado donde presente la vulnerabilidad.

Por lo que se puede concluir, “la auditoría en un sistema operativo, se puede utilizar para la identificación de actividades maliciosas del usuario, investigación forense del sistema y el cumplimiento de la seguridad informática” (Mistry, 2018, pág. 12), y a través de controles que son mostrados en las diferentes categorías y adoptados de manera preferente por la institución, empresa o negocio que requiere de este proceso, se evitaría la vulnerabilidad de su sistema automatizado de información.

El uso de las Tecnologías de la Información y Comunicación en las instituciones públicas.

La Constitución de la República del Ecuador en su artículo 66.19 garantiza a las personas "el derecho a la Protección de Datos de carácter personal, que incluye el acceso y la decisión sobre la información y datos de este carácter, así como su correspondiente protección, recolección, archivo, procesamiento, distribución o difusión de estos datos, información que requerirá la autorización del titular y el mandato de la ley" (Asamblea Nacional Constituyente CRE, 2008, pág. 23) (Asamblea Nacional Ley Orgánica de Transparencia y Acceso a la Información Pública, 2021).

La Ley Orgánica de Transparencia y Acceso a la Información Pública, la cual fue publicada en el Registro Oficial 337 del 18 de marzo de 2004, establece en aquella parte fundamental referente a los datos personales y a las tecnologías de la información y comunicación, "que esta ley garantiza el derecho fundamental de las personas a la información" (Asamblea Nacional Ley Orgánica de Transparencia y Acceso a la Información Pública, 2021, pág. 1).

En esta misma ley, en su artículo uno dispone: "los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación del servicio electrónico a través de redes de información, incluyendo el correo electrónico y la protección de los usuarios de estos sistemas", son responsabilidad del Estado y garantiza el acceso de sus titulares a la información que se encuentra navegando por la red, lo cual es concordante con lo que establece el artículo 9 y sobre la Protección de Datos y transmisión de mensajes, en el que "se requerirá el consentimiento expreso del titular, quién podrá seleccionar la información a compartirse a terceros" (Asamblea Nacional Ley Orgánica de Transparencia y Acceso a la Información Pública, 2021, pág. 3); además, también garantiza en la misma disposición legal antes anotada, "que la recopilación y el uso de datos personales, responden a los derechos de privacidad, intimidad y confidencialidad, garantizados en la Constitución, y esta ley, los cuales podrán ser utilizados o transferidos únicamente

con autorización del titular u orden de autoridad competente" (Asamblea Nacional Ley Orgánica de Transparencia y Acceso a la Información Pública, 2021, pág. 5).

De la misma manera, en el artículo 66 de la Carta Fundamental, se encuentra garantizada la seguridad de la información, en la que se dispone de manera categórica la protección de aquellos datos personales de todo ciudadano, tanto nacional como extranjero, o de aquellos que viven dentro de las jurisdicciones territoriales del Ecuador o sometidos a las mismas.

El artículo 5 de la Ley de Comercio Electrónico dispone "que los mensajes de datos cualquiera que sea su formato medio o intensión, deberán responder a los principios de confidencialidad y reserva" (Asamblea Nacional Ley de Comercio Electrónico, 2021, pág. 3), entendiéndose por tal el hecho de que toda la información que se encuentra en los sistemas automatizados de información y que cuente con la protección del Estado que no sean públicos, tendrán una categoría de reservados y confidenciales; esto significa, que solamente tendrá acceso el titular de la misma, o a quien éste haya dado los permisos para que puedan acceder a la información, y usarla de la manera que haya sido dispuesta por el titular, estableciendo así, de manera clara y precisa, la prohibición del acceso no consentido a estos sistemas y redes telemáticas de información.

El artículo 7 de la misma ley garantiza la integridad de los datos informáticos, detallando que "se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable en su contenido, salvo algún cambio de forma propia del proceso de comunicación, archivo y presentación" (Asamblea Nacional Ley de Comercio Electrónico, 2021, pág. 3).

Finalmente, el artículo 8 de la ley de Comercio electrónico establece la garantía de la disponibilidad de los datos personales, manteniendo las siguientes condiciones:

"a) Que la información que se contenga en un mensaje de datos, sea accesible para su posterior consulta.

b) Que se haya conservado el formato en el que se ha generado, enviado, recibido o cuando algún formato que sea demostrable y que se produce con exactitud en la información generada, enviada o recibida.

c) Que se conserve todo dato que permite determinar el origen y el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado" (Asamblea Nacional Ley de Comercio Electrónico, 2021, pág. 4).

De lo anteriormente enunciado, se puede establecer que efectivamente en la República del Ecuador se encuentra garantizado el uso de las tecnologías de la información y comunicación, con la Protección de Datos personales así como de la confidencialidad, integridad y disponibilidad de datos, en aquellos sistemas automatizados de información que sean configurados de acuerdo a las necesidades que tenga cada una de las instituciones, pero que dentro del mismo, se proteja la información que se encuentra resguardada bajo la Ley de Acceso a la Información Pública.

Es necesario aclarar, que efectivamente esta ley garantiza que toda información tiene que estar accesible al público en general, a excepción de aquella que tiene la categoría de reservada; sin embargo, se debe explicar que tratándose de los sistemas automatizados de información, esta tiene dos partes. La primera parte que es manejada por el administrador del sistema, o por aquella persona que construye el software en atención a las necesidades que tiene la institución pública que presta servicio a la comunidad, y que solamente tiene acceso el administrador, o aquellas personas a quienes se les haya dado la autorización para el manejo de los subsistemas que permiten la operatividad del mismo. La segunda parte corre a partir de la ejecución del programa en la que el operador de ventanilla, o el especialista que realiza la atención al usuario, ingresa al sistema para poder prestar el servicio de acuerdo a la funcionalidad de este.

Un ejemplo es el Sistema Automático de Trámite Judicial Ecuatoriano SATJE, el cual pertenece al Consejo Nacional de la Judicatura que tiene varios módulos, entre ellos el de sorteo de causas,

módulo de administración, quienes tienen acceso único para el manejo de todo el sistema operativo, así como la Dirección Nacional de Talento Humano, las Direcciones Provinciales del Consejo de la Judicatura, la Dirección Nacional de Gestión Procesal, etc., los que dentro de sus funcionalidades tienen registrados usuarios con su respectiva identificación y control de acceso y movimientos dentro de las aplicaciones y programas; ya que se les entrega un usuario y contraseña, los que tienen permisos para habilitar o deshabilitar ciertas funcionalidades operativas ya en la ejecución del mismo, y por lo que se puede observar, este fue programado para prestar servicios específicas para la correcta administración de justicia en el Ecuador, cubriendo desde las TICs todas las necesidades reglamentarias que la ley exige.

Se puede establecer, que efectivamente el software funciona conforme éste haya sido configurado, y el responsable del mismo es el administrador del sistema, que si bien es cierto no pueda presentar ninguna clase de hackeo a las medidas de seguridad impuestas que presenten alguna intromisión o ataque al mismo, si puede presentar un exceso en la autorización para poder manejar el sistema o subsistema ejecutando una tarea diferente a la que se encuentra detallada en la ley.

El *iter críminis*, las TICs y el favorecimiento por el desconocimiento del funcionamiento del sistema.

El funcionamiento de un sistema informático se encuentra sustentado en 3 grandes acciones; la introducción de información a través de los sistemas periféricos como son el teclado, los puertos USB que son puertos físicos del hardware para que la información que ha sido introducida a través de estos medios electrónicos, pueda ser procesada a través de la organización, almacenamiento y transformación que para el efecto se realiza en el interior del ordenador, y finalmente, esta información de salida, lo cual es la respuesta que para el efecto realiza el sistema operativo central, a través de un software “el cual es un conjunto de programas cuya finalidad es lograr la ejecución de

tareas específicas requeridas por el usuario del sistema, bien sea por medio de interacción entre este y el hardware, o entre el software del sistema operativo y otras aplicaciones del mismo" (Parilli, 2020, pág. 3).

El administrador de un sistema informático tiene como responsabilidad:

a) Administración del hardware del sistema operativo, así como de las aplicaciones instaladas que prestan las facilidades para el usuario final, y para el administrador del mismo.
b) La administración de los usuarios.
c) Comprobar que el sistema esté presentando un buen funcionamiento conforme ha sido configurado en el momento oportuno.
d) Administrar los procesos de seguridad de la información y de la seguridad informática, mediante un procedimiento de hardening en la que se robustecen las medidas de seguridad que han sido impuestas para evitar la intromisión al sistema operativo.

Bajo lo explicado, se encuentra la alteración, manipulación o modificación de los datos informáticos cuando accede al sistema operativo el *insider hacker*, quién es el que cambia la funcionalidad del sistema, para que realice una tarea totalmente distinta a la que fue legalmente autorizada. Esta es la razón por la que se puede entender, que el exceder en la autorización conferida por el titular al administrador del sistema o subsistema en la funcionalidad del mismo, afectaría al usuario final, y por ende, se estaría cometiendo algún acto ilícito.

Los sistemas están configurados para que presenten una funcionalidad específica de acuerdo a las necesidades de la institución. Esta funcionalidad se encuentra establecida de acuerdo al orgánico funcional que para el efecto tenga esta institución del Estado, quien presta un servicio a la sociedad, o para administrar ciertos perfiles o ciertas tareas que han sido destinadas para una situación en especial.

La presentación de estos actos presuntamente delictivos, presentan un problema al momento de su descubrimiento, en virtud de que es mucho más compleja esta clase de infracción informática que las tradicionales, ya que necesitan para la comisión del injusto penal, de personas con conocimientos técnicos-científicos relativos a la informática, y que necesitan obligatoriamente de personal especializado que realice la investigación en uso de las TICs.

En las fases del *iter críminis*, al ejecutar los actos preparatorios, la conducta de exceso en la autorización concedida por el titular para acceder al sistema, se encuadra al injusto penal, cuando este altera, manipula o modifica el mismo a su conveniencia y para su propio beneficio, de allí que se consuma cuando este ha ejecutado la tarea que fue configurada dolosamente; razón por la cual, el desconocimiento por parte del usuario final de las TICs y de la forma como se encuentra establecida y configurada la funcionalidad del sistema, es un factor preponderante para así poder llegar a determinar la autoría y participación de la persona que haya actuado dolosamente en la comisión del acto lesivo.

En atención al abordaje dado al *iter críminis*, se puede establecer que las conductas en las cuales excede la autorización conferida por el titular al administrador del sistema, o aquella persona que tiene la autorización para manejar los subsistemas operativos desarrollados para presentar la funcionalidad del mismo, se encuentran encasillados a partir de los actos de ejecución.

Los actos de corrupción en la administración pública.

Conforme se encuentra establecido en el artículo 227 de la Constitución de la República del Ecuador que ordena, que “la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación” (Asamblea Nacional Constituyente CRE, 2008, pág. 30), se puede colegir, que todos los funcionarios que prestan sus

servicios en las instituciones del Estado, se encuentran en la obligación de ejercer sus funciones con honestidad, honradez y buen servicio a la comunidad, y no realizar actos que puedan ser considerados contrarios a derecho, y que definitivamente vayan a terminar con la consumación de algún acto tipificado como delito en el ordenamiento punitivo ecuatoriano.

En el artículo 83 numeral 8 del mismo texto legal invocado establece como deber y responsabilidades para todos los ecuatorianos y ecuatorianas, el "administrar el patrimonio público honradamente y con apego irrestricto a la ley" (Asamblea Nacional Constituyente CRE, 2008, pág. 27), lo que denota que efectivamente todos los servidores públicos están obligados a dar cumplimiento a la ley, conforme lo dispone el artículo 233 ibídem, en el que detalla "que ningún servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones o por omisiones" (Asamblea Nacional Constituyente CRE, 2008, pág. 34), por lo que incurrirán en responsabilidades civiles, penales y administrativas por la administración de fondos, bienes o recursos públicos.

Así también, la Convención de las Naciones Unidas contra la Corrupción y la Convención Interamericana contra la Corrupción, constituyen una norma que ha sido suscrita por el Estado ecuatoriano con la finalidad de establecer prevención y represión de actos irregulares cometidos por servidores públicos, que de una u otra manera, se encuentran laborando al servicio del Estado y realizan actos de corrupción, en virtud de que estarían violentando las responsabilidades que le han sido entregadas, ya sea por nombramiento provisional, nombramiento definitivo o mediante contrato con obligaciones de servicio a la comunidad a la que pertenecen.

En atención a lo manifestado y en base a la investigación realizada, se puede llegar a colegir que efectivamente son actos de corrupción, cuando el servidor público con responsabilidad de administrador del sistema u otra persona con la misma responsabilidad, exceden la autorización conferida por el titular, quien tiene la representación legal de la institución Estatal, y ejecuta desde las TICs una tarea diferente para beneficiar a si mismo o un tercero, por lo que incurriría en el tipo

penal contra la eficiencia de la administración pública, descrito y sancionado en el artículo 285 del Código Orgánico Integral Penal (Código Orgánico Integral Penal., 2014), que sanciona el tráfico de influencias, a más de otros delitos que tienen que ver con el uso de las TICs, y que llevan inmerso en los elementos descriptivos y normativos del tipo objetivo, la alteración modificación y manipulación de datos de un sistema automatizado de información.

Se habla de la adecuación típica al delito de tráfico de influencias ya que este en su tipo objetivo, exige que esta persona tenga la categoría de servidor público, y que trabaje en alguna de las instituciones del Estado que para el efecto se encuentran establecidas en la Constitución de la República del Ecuador, y que valiéndose del cargo o facultad que le da el mismo, o que se encuentre derivada de aquella relación personal o jerárquica que le otorga su nombramiento o su contrato, ejerza influencia en otro servidor para tener algún acto o resolución que genere beneficio personal material o inmaterial o a un tercero.

Si este servidor público ejecuta dentro del sistema automatizado de información alguna funcionalidad que derive en un acto de corrupción, en el cual va a beneficiar a una tercera persona, o deja de hacer algo que para el sistema se encontraba configurado, y este responda de una manera específica que atente a los intereses institucionales, estaría incurriendo en la disposición legal antes anotada, o en cualquiera de los tipos penales informáticos que para el efecto se encuentran tipificados en el Código Orgánico Integral Penal, que describen y sancionan la alteración, modificación o manipulación de los sistemas informáticos.

Estos sistemas han sido programados con la finalidad de prestar ciertas funcionalidades operativas, cuyo software ha sido programado de acuerdo a las necesidades que tenga esta institución, y en este caso, las TICs generan en favor de la administración pública, mucha más celeridad y buen servicio en favor de la ciudadanía.

Los servidores públicos que tienen permisos de administrador y las claves de acceso para el manejo del sistema, son los encargados de prestar un buen servicio en uso de las tecnologías de la información y comunicación, y evitar la alteración, manipulación o modificación de datos informáticos que puedan cambiar la funcionalidad del sistema operativo, por lo que es necesario realizar auditorías de control de acceso, así como establecer mayores medidas de seguridad que no solamente le permitan al administrador manejarlo, sino también que el titular de las cuentas tenga acceso, con la finalidad de evitar esta clase de actos delictivos que afectan a la administración pública y que terminan en actos de corrupción que se encuentran debidamente sancionados en nuestra ley penal.

Se justifica, que la falta de medidas de seguridad, auditoría y control de los sistemas automatizados de información, permiten su alteración, modificación y manipulación de datos informáticos, permitiendo así la ejecución de diferentes conductas contrarias a derecho en beneficio de terceros, perjudicando a la institución pública dueña del sistema, razón por la cual denota la importancia del fortalecimiento de estas medidas de seguridad informática y de la información, y así evitar ser víctimas de estos actos de corrupción.

CONCLUSIONES.

Al término de la presente investigación, se arriba a las siguientes conclusiones:

- La sociedad de la información es un referente de desarrollo en todas sus clases, social, cultural, político, empresarial, financiero, jurisdiccional, obligando al ser humano a intercambiar datos para un desarrollo personal, profesional y social en uso de las Tecnologías de la Información y las Comunicaciones.
- La República del Ecuador ha garantizado el uso de las Tecnologías de la Información y las Comunicaciones con la protección de datos personales, así como de la confidencialidad,

integridad y disponibilidad de datos, en las instituciones públicas como privadas, de acuerdo a las necesidades inherentes a sus misión y visión.

- Se ha podido llegar a establecer que la conducta de hackeo no solo aborda la vulneración de las medidas de seguridad de los sistemas automatizados de información, sino también, cuando se excede en la autorización dada por el titular para poder acceder a ese sistema de manera dolosa.
- En atención a esto, se puede establecer, que la conducta de exceso en la autorización conferida por el titular al administrador del sistema operativo se consuma cuando se ejecutó alguna alteración, modificación o manipulación del sistema automatizado de información, para que presente una tarea diferente a la que se encuentra configurada legalmente, o deje de hacer una tarea para la que ha sido establecida y beneficiarse de la misma para si o un tercero.
- Que los actos de corrupción derivados del uso de las Tecnologías de la Información y las Comunicaciones en las instituciones del Estado, se les puede verificar cuando existe alteración, manipulación o modificación de los datos de un sistema automatizado de información para haga o deje de hacer alguna terea que beneficie a sus intereses o de terceros.
- Que el proceso de hardening al ser un procedimiento que robustece las medidas de seguridad informática y de la información, es el mejor método para reducir las vulnerabilidades que presenta al sistema.

REFERENCIAS BIBLIOGRÁFICAS.

1. Aboso, G. (2017). Derecho Penal Cibernético. La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación. Buenos Aires: Editorial BdeF. Ltda.

2. Abdel-Aal, S. I., Abd-Ellatif, M. M. A., & Hassan, M. M. (2018). Two Ranking Methods of Single Valued Triangular Neutrosophic Numbers to Rank and Evaluate Information Systems Quality. Neutrosophic Sets and Systems, 9, 132–141.
3. Ardila, J., Salcedo, F., Pedraza, C., & Saavedra, M. (2020). Revisión sobre Hacking ético y su relación con la inteligencia artificial, . Revista RETO, volumen 8, núm. 1; enero-diciembre 2020, ISSN 2333-8059.
4. Asamablea Nacional Ley Organica de Transparencia y Acceso a la Información Pública. (2021). Ley Organica de Transparencia y Acceso a la Información Pública. Quito: Corporación de Estudios y Publicaciones.
5. Asamblea Nacional Constituyente CRE. (2008). Constitución de la República del Ecuador. Montecristi: Corporación de Estudios y Publicaciones.
6. Asamblea Nacional Ley de Comercio Electrónico. (2021). Ley de Comercio Electronico, Firmas y Mensajes de Datos. Quito: Corporacion de Estudios y Públicaciones.
7. Busón, C. (2020). La minería de opinión para el análisis del discurso de odio en las redes sociales. Un estudio de caso sobre Paulo Freire en YouTube durante el periodo 2007-2019. . Commons. Revista de Comunicación y Ciudadanía Digital, 9(1), 119–159. https://doi.org/http://doi.org/10.25267/COMMONS.2020.v9.i1.5
8. Centro de innovación y soluciones empresariales y tecnológicas. (28 de Mayo de 2020). Centro de innovación y soluciones empresariales y tecnológicas. Obtenido de CISET: https://www.ciset.es/publicaciones/blog/746-hardening
9. CEPAL. (2013). Los caminos hacia una sociedad de la información en America Latina y el Caribe. Comision Económica para America Latina y el Caribe, 27.
10. Cobo Romani, J. (2009). El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. Revista Zer, 312.

11. Código Orgánico Integral Penal. (2014).
12. Desongles Corrales, J. y. (2006). Conocimientos Básicos de la Informática. Sevilla : Editorial MAD.
13. Diario El Pais. (30 de agosto de 2021). Dario El Pais. Obtenido de Diario El Pais: https://elpais.com/noticias/kgb/
14. Gómez, Á. (2014). Enciclopedia de la seguridad Informática. Mexico: Editorial Alfaomega,.
15. González Pérez, P. (2015). Pentesting persistente y estrategico: nuevos ataques y nuevos modelos. Red de seguridad, 66-68.
16. González, R. (9 de junio de 2019). eHack. Obtenido de eHack, Retrieved 06 29, 2020, from las fases del hacking ético: https://ehack.info/las-fases-del-hacking-etico/
17. Falcón, V. V., Espinoza, J. L. T., Yacelga, A. R. L., & Zambrano, L. O. A. (2021). Managing Contradictions in Software Engineering Investigations using the Neutrosophic IADOV Method. Neutrosophic Sets and Systems, 44, 100–107. https://doi.org/DOI: 10.5281/zenodo.5162566
18. Hilbert, M. (2009). La sociedad de la información en América Latina y el Caribe. Desarrollo de las tecnologías y tecnologías para el desarrollo. Santiago de Chile: Ediciones CEPAL, Comisión Económica para América Latina y el Caribe.
19. Historia de redes informaticas. (27 de enero de 2018). Redes informaticas. Obtenido de Redes informaticas: https://redesinformaticas981.wordpress.com/historias-de-redes-informaticas/
20. Kurzweil, R. (1999). The Age of Spiritula Machine: When Computers Exceed Human Intelligence. Nwe York: Viking.
21. Mistry, S. (2018). Endpoint Protection through Windows Operating. International. Semantic Scholar. doi:DOI:10.7753/IJCATR0702.1005
22. Morgan, L. H. (1877). Ancient Society. New York: H. Holt and company. .

23. Pacheco, S. (2009). Una metodología efectiva para la Priorización de Proyectos en TIC. Sistemas, Cibernética E Informática, 6(2), 23–28.
24. Parilli, M. (06 de Mayo de 2020). Tecno informatica, ¿Como funciona el software?. Obtenido de Tecno informatica. https://tecnoinformatic.com/c-informatica-basica/como-funciona-el-software/
25. Programa de las Naciones Unidas para el Desarrollo. (2002). Informe sobre Derecho Humano en Vnezuela 2002. Las Tecnologías de la Información y Comunicación al servicio del desarrollo. Caracas: PNUD.
26. Quiroz Martinez, M. A., Mayorga Plua, S. E., Gomez Rios, M. D., Leyva Vázquez, M. Y., & Plua Morán, D. H. (2020). Chatbot for Technical Support, Analysis of Critical Success Factors Using Fuzzy Cognitive Maps. International Conference on Applied Technologies, 363–375.
27. Suarez, A. (2016). Manual de delito informático en Colombia. Análisis dogmático de la ley 1273 de 2009,. Bogotá: Universidad Externado de Colombia.
28. Vásquez, R. A. D., Jadan, B. E. V., & Caballos, C. Y. D. (2021). Dionisio Vitalio Ponce Ruiz, Neutrosophic Statistics in the Strategic Planning of Information Systems. Neutrosophic Sets and Systems, 44, 402–410. https://doi.org/DOI: 10.5281/zenodo.5163680

DATOS DE LOS AUTORES.

1. **Alberto Leonel Santillán Molina.** Magister en Derecho Penal y Criminología. Fiscal Provincial de Pichincha y Profesor Titular Principal de la Universidad Regional Autónoma de los Andes, con correo electrónico: us.albertosantillan@uniandes.edu.ec
2. **Nelly Valeria Vinueza Ochoa.** Magister en Derecho Constitucional. Funcionaria de Secretaría de la Fiscalia General del Estado y Docente de la Universidad Regional Autónoma de los Andes, con correo electrónico: ub.nellyvinueza@uniandes.edu.ec

3. **Cristian Fernando Benavides Salazar.** Magister en Derecho Constitucional. Docente de la Universidad Regional Autónoma de los Andes, con correo electrónico: us.cristianbenavides@uniandes.edu.ec

RECIBIDO: 1 de agosto del 2021. **APROBADO:** 3 de septiembre del 2021.