



LA IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA EN LAS INSTITUCIONES GUBERNAMENTALES (ECUADOR)

Master, Pablo Adriano Alarcón Salvatierra

Master, Ronald Alfredo Barriga Díaz

Master, Christian Omar Picón Fara

Master, José Abel Alarcón Salvatierra

Docentes de la Facultad de Matemáticas y Física – Universidad de Guayaquil (FCMF). Guayaquil, Ecuador.

pablo.alarcons@ug.edu.ec

ronald.barrigad@ug.edu.ec

christian.piconf@ug.edu.ec

abel.alarcons@ug.edu.ec

Para citar este artículo puede utilizar el siguiente formato:

Pablo Adriano Alarcón Salvatierra, Ronald Alfredo Barriga Díaz, Christian Omar Picón Fara y José Abel Alarcón Salvatierra (2016): "La importancia de la seguridad informática en las instituciones gubernamentales (Ecuador)", Revista Caribeña de Ciencias Sociales (noviembre 2016). En línea:

<http://www.eumed.net/rev/caribe/2016/11/seguridad.html>

RESUMEN

La seguridad es una parte fundamental en redes y comunicaciones, por lo cual se necesita tener soluciones rápidas y sobre todo eficientes que ayuden a gestionar de manera eficaz amenazas informáticas que atentan contra la disponibilidad de servicios, integridad de la información y confidencialidad de los datos. El objetivo principal es robustecer el sistema para así evitar ataques y que existan vulnerabilidades que en algún momento lleguen a dañar los servidores, pérdida o alteración información como datos personales de quienes usen el sistema. Además, siguiendo estándares y recomendaciones para lograr un óptimo esquema de seguridad y no llegue existir ninguna falencia.

PALABRAS CLAVES: Seguridad, Hardening, vulnerabilidades, ataques informáticos y amenazas.

SUMMARY

Safety is a key part of networking and communications, so you need to have fast and above all efficient solutions that help effectively manage threats that threaten the availability of services, information integrity and confidentiality of data. The main objective is to strengthen the system to avoid attacks and vulnerabilities that exist at some point reach servers damage, loss or alteration information as personal data of those using the system. Furthermore, following standards and recommendations for optimal security scheme and arrive be no flaw.

KEYWORDS: Security, hardening, vulnerabilities, computer attacks and threat.

I.- INTRODUCCIÓN

El avance tecnológico que se ha producido en los últimos años y específicamente de las redes informáticas, ya sea un dispositivo móvil o fijo ha ocasionado el desarrollo de software y levantamiento de servidores sea cada vez más constante y cotidiano, por lo cual se manejan cronogramas, horarios, fechas de cumplimientos y entre otros aspectos que hacen que se busque la funcionalidad por encima de la seguridad, lo cual no es malo, pero sin embargo, debe de considerarse aspectos tales como codificaciones seguras, buenas prácticas y entre otros temas los cuales eviten dejar vulnerabilidades de seguridad que pueden ser explotadas en posibles ataques informáticos.

En las instituciones gubernamentales la seguridad informática es uno de los requerimientos más importante ya que en la mayoría de las aplicaciones y servicios que se brindan a la ciudadanía, no se toman en cuenta medidas de seguridad o análisis de posibles puntos débiles.

Toda institución gubernamental que no cuente con un esquema de seguridad establecido, siempre será un fácil objetivo para terceras personas conocidas como cibercriminales que aprovechan las vulnerabilidades de los sistemas para obtener información que pueden involucrar datos de tipo sensibles, críticos y confidenciales de los ciudadanos y de las operaciones de la institución. Por lo cual surge la necesidad, que toda institución pública u otras organizaciones deben manejar un ciclo de mejora continua en los procesos de seguridad implementados.

II.-ANTECEDENTES

Toda organización debería contar con una línea base de seguridad para sus equipos productivos, la cual los lleve a un nivel mínimo satisfactorio de seguridad a través de un proceso de Hardening. Un análisis de vulnerabilidades, por su parte, tiene como objetivo identificar huecos de seguridad y medir el impacto sobre los activos, y utiliza los hallazgos para visualizar cuáles serían las siguientes acciones para fortalecerlos y puedan soportar ataques a los que podrían estar expuestos.¹
(Sánchez, 2013)

Dado que los lineamientos bases de seguridad, no son un proceso estático, sino más bien un proceso cíclico de mejora continua, es preciso realizar diversas actividades que mitiguen diversas vulnerabilidades que se presenten en la TIC (Tecnología de la Información).

En algunos países la seguridad institucional es considerada como seguridad nacional, por lo expuesto se debe contar con un documento de políticas de seguridad, el mismo que debe plasmar mecanismos confiables que protejan los activos tecnológicos.²

Este estudio realizado en el 2014 habla sobre la necesidad de definir un manual de políticas de seguridad, la falta de políticas de seguridad aumenta el riesgo de vulnerabilidades, por lo cual al definir estas políticas proporcionará un control confiable de los activos informáticos de las instituciones públicas, estas políticas siempre deben basarse en normas internacionales tales como ISO/ICE 27000, OWAS, COBIT, entre otras.

La seguridad informática se debe considerar como un tema importante para las entidades por lo que no debe aislarse de los demás procesos que se manejan en ella, debido a que la información está expuesta a diferentes amenazas y vulnerabilidades. Es un conjunto de elementos físicos y lógicos dedicados a

¹ <http://www.magazcitum.com.mx/?p=2109#.V5wBkfnhCM8>

² <http://repositorio.uteq.edu.ec/bitstream/43000/130/1/T-UTEQ-0010.pdf>

imposibilitar el acceso a un sistema informático a todo aquel que no se encuentra autorizado, brindando protección a la infraestructura tecnológica. Para lograr la seguridad en los sistemas se debe implementar un conjunto de controles en software, hardware, políticas de control y acceso.³

Esta investigación hace referencia a la importancia de la seguridad informática que debería tener toda institución pública para lograr una eficiente administración de sus activos físicos y lógicos la cual tiene que ser rápida, segura y centralizada, para lograr un buen sistema de seguridad, se apoya en el concepto de Hardening que es un proceso que fortalece al máximo posible la seguridad de un sistema informático y disminuyendo los riesgos de posibles amenazas de ataques informáticos.

En los sistemas informáticos actuales prácticamente no existe el concepto de ordenador aislado como sucedía en ordenadores de generaciones anteriores, sino que es extraño un sistema informático que no esté dentro de una red de ordenadores para compartir recursos e información, así como acceso a internet, por lo cual las amenazas les pueden llegar desde el interior, así como desde el exterior, y al estar conectado en red, un ataque a un equipo, puede afectar a todo el conjunto.⁴

Hoy en día todo sistemas informático está conectado en una red interna o a internet con la finalidad de compartir recursos entre otros ordenadores o sistema de cómputo, por lo cual los riesgos de amenazas de ataques pueden aumentar, estas amenazas pueden producirse tanto desde el exterior como del interior este es una de las razones más importantes para implementar un esquema de seguridad ya que cualquier ataque al estar conectado en red puede comprometer a todo un conjunto de sistema informático.

³ <http://www.eumed.net/rev/cccss/2016/02/servicios.html>

⁴

<https://books.google.com.ec/books?id=c8kni5g2Yv8C&printsec=frontcover&dq=seguridad+informatica&hl=es&sa=X&ved=0ahUKEwj2q6zYvdvOAhUDGh4KHRhGBt0Q6AEIMTAD#v=onepage&q=seguridad%20informatica&f=false>

III.- CARACTERISTICAS

PILARES FUNDAMENTALES DE LA SEGURIDAD INFORMÁTICA

Seguridad informática⁵

“La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.” (López, 2010)

Dando a entender que la seguridad informática nos dará a conocer si un sistema está en peligro, en riesgo o sufrió algún daño; para luego mediante procedimientos obtener un sistema seguro.

CLASIFICACIÓN DE LA SEGURIDAD INFORMÁTICA

Seguridad Física: Consiste en la protección dentro del Centro del cómputo es decir todo el hardware y los medios de almacenamiento. Donde se debe tener en cuenta:

- Desastres
- Incendios
- Equipamiento
- Inundaciones
- Picos y ruidos electromagnéticos
- Cableado

Seguridad Lógica: Consiste en la protección de los sistemas, información almacenada, procesos y servicios; siguiendo procedimientos que aseguren que sólo personal autorizado va a tener acceso. Donde se debe tomar en cuenta:

- Controles de acceso
- Identificación
- Roles
- Transacciones
- Limitaciones a los servicios

Aspectos fundamentales de seguridad

La seguridad tiene tres aspectos fundamentales que van ligados con los objetivos que los atacantes intentan vulnerar y son los siguientes: confidencialidad, integridad y disponibilidad. En base a estos aspectos fundamentales, el atacante encontrara y explota las vulnerabilidades del sistema.

- **Confidencialidad:** garantizar que la información solo sea accedida por personal autorizado.
- **Integridad:** asegurar que la información no sea alterada por ningún individuo o entidad externa.
- **Disponibilidad:** garantiza que la información sea accedida por personal autorizado ya sea en cualquier lugar o momento cuando se lo requiere.

Amenazas

La amenaza es aquella que atenta contra la seguridad de la información, siempre va existir una amenaza si llega haber alguna falencia es decir vulnerabilidad y causara daño (material o inmaterial) en los elementos del sistema quebrantando los aspectos fundamentales de seguridad ya sean confidencialidad, integridad, disponibilidad.

Vulnerabilidad

Las vulnerabilidades son las debilidades de un sistema informático que permitirán a un atacante causar daño, estas vulnerabilidades pueden aparecer tanto en el hardware como el software. Además, las vulnerabilidades tienen relación con las amenazas, es decir si no hay amenaza no existirá vulnerabilidad.

Las vulnerabilidades se pueden descubrir por medio de un análisis de vulnerabilidades. Este análisis nos dará a conocer el estado y la seguridad del equipo, red y del sistema, en el cual se obtiene un informe y hasta a veces como corregir dicha vulnerabilidad para reducir la falla que se detectó.

Riesgos

Es la posibilidad de que se produzca una amenaza y luego se pueda producir un ataque. Los riesgos serían una probabilidad de que suceda un ataque en base a la amenaza. Analizando los riesgos de un sistema se puede conocer el impacto que tendrá y así tomar decisiones para proteger el sistema.

Ataques Informáticos

Los ataques informáticos tratan de aprovechar las debilidades o fallas en el hardware, software o también a las personas que trabajan directamente en el ambiente para así obtener beneficios, la mayoría para obtener dinero afectando negativamente la seguridad del sistema.

Anatomía de un ataque informático

Hay que conocer las diferentes etapas que comprende un ataque informático, obteniendo así una gran ventaja de comprender la forma de pensar como un atacante. Desde el punto de vista profesional hay que aprovechar estas habilidades para conocer y aprender de qué manera los ataques actúan.

Gráfico N° 1

Anatomía de un ataque informático



Fuente: https://www.evilmfingers.com/publications/white_AR/01_Atques_informaticos.pdf

Elaborado por: Ingrid Espinoza Robles, Vicente Cevallos Cedeño, Melissa Andrade Ureta, José Bonilla Lastra, Jefferson Montes Briones

Fase 1: Reconocimiento. En esta etapa se realiza la recolección de información con respecto a la víctima ya sea una persona o institución.

Además, para obtener dicha información se apoya en internet a través de buscadores como Google. Entre las técnicas más utilizadas se encuentran ingeniería social y el sniffing.

Fase 2: Exploración. En esta etapa según la información adquirida en la fase 1 se realiza un sondeo y así obtener información del sistema como direcciones IP, datos de autenticación, entre otros.

Para adquirir información del sistema se lo hace mediante herramientas como: escáneres de redes, escáneres de puertos, escáneres de vulnerabilidades, port mappers.

Fase 3: Obtener acceso. Una vez conocidos todas las vulnerabilidades se las explota y también los fallos del sistema que se encontraron en las fases de reconocimiento y exploración.

Entre los ataques que el hacker puede realizar están ataques de denegación de servicio (DoS), ataques distribuidos de denegación de servicio, filtrado de contraseñas, entre otros.

Fase 4: Mantener el acceso. Luego de haber accedido al sistema, se tratará de implantar herramientas para que así pueda el atacante ingresar en un futuro desde cualquier parte que se encuentre. Para poder mantener ese acceso los atacantes utilizan troyanos, rootkits y backdoors.

Fase 5: Borrar huellas. Luego que el atacante logró extraer y mantener acceso al sistema, comenzará a borrar las evidencias que se dejó para que así no ser detectado por el personal de seguridad o administradores.

DEBILIDADES DE SEGURIDAD COMÚNMENTE EXPLOTADAS

Entre las debilidades que saben explotar los ataques tenemos las siguientes:

Ingeniería social⁶

“Si bien esta técnica es utilizada en cualquier ámbito, en lo que a informática se refiere, consiste en la obtención de información sensible y/o confidencial de un usuario cercano a una sistema u organización explotando ciertas características que son propias del ser humano.” (Mieres, 2009)

El mayor problema de seguridad en informática dentro de una organización son las personas ya que son capaces de decidir si quebrantar las reglas establecidas en las políticas de seguridad.

⁶ https://www.evilmfingers.com/publications/white_AR/01_Atques_informaticos.pdf

Para poder resolver este problema es la educación, desde la secretaria, administradores de red, hasta los grandes jefes deberían estar capacitados acerca de las debilidades y engaños que más se utilizan por los atacantes para que así pueden identificarlos y poder avisar si existe algún inconveniente en el equipo.

Factor insiders

La mayoría piensa que los ataques lo realizan personas ajenas a una organización es decir alguien totalmente desconocido que hace ataque desde un lugar remoto a altas horas de la noche. Aunque no es tan cierto, ya que también se realizan violaciones de seguridad dentro de la organización y por empleados conocidos como Factor Insiders.

Esto puede suceder que un empleado está molesto, decide robar información y causar daños para tomar venganza para obtener dinero a través de la información de la organización y se lo conoce como Insiders Trading.

Aunque se llegue a implementar muchas medidas de seguridad no podrán ser eficaces, por lo que se debe tomar otras medidas como, por ejemplo: instalar programas adicionales keyloggers que monitorean continuamente el sistema de qué es lo que se hace exactamente, estricta configuración a nivel de privilegios, deshabilitación de puertos USB y entre otros.

Códigos maliciosos ⁷

“Esta amenaza se refiere a programas que causan algún tipo de daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.” (Mieres, 2009)

Este tipo de ataques son los que más se dan ya que se realizan a través de programas troyanos. Este troyano ingresa al sistema de manera silenciosa y activa una carga perjudicial o también son usados de manera combinada con otros códigos maliciosos que ayudan a esconder huellas que el hacker deja en el sistema y también deja backdoors para luego ingresar de nuevo cuando lo desee.

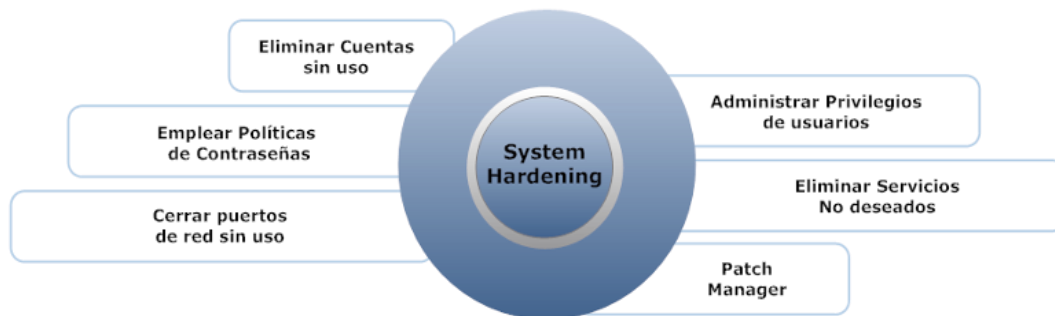
⁷ https://www.evilmfingers.com/publications/white_AR/01_Atques_informaticos.pdf

Hardening

Hardening es poner las cosas más complicadas a quien te va a robar la información o quien te la va a cambiar, es hacer que un sistema sea más robusto, tenga menos servicios abiertos, este más optimiza do desde el punto de vista de la disponibilidad y evitar el acceso no autorizado.

GRÁFICO 2

Sistema de hardening



Elaboración: Autores

Fuente: <http://www.caberseg.es/detalle.php?nid=29>

El Hardening ayudará a proteger la integridad, la disponibilidad, confidencialidad de la información que se encuentra alojada en el hardware.

Eduardo Sánchez dice que toda organización debería contar con una línea base de seguridad para sus equipos productivos, la cual los lleve a un nivel mínimo satisfactorio de seguridad a través de un proceso de Hardening. Un análisis de vulnerabilidades, por su parte, tiene como objetivo identificar huecos de seguridad y medir el impacto sobre los activos, y utiliza los hallazgos para visualizar cuáles serían las siguientes acciones para

fortalecerlos y puedan soportar ataques a los que podrían estar expuestos.⁸ (Sánchez, 2013)

Niveles de profundidad del Hardening

GRÁFICO 3

Niveles de profundidad del Hardening



Elaboración: Autores

Fuente: <http://www.magazcitum.com.mx/?p=2109#.V7-lyZjhBhE>

Fortalecimiento a nivel de host

Básicamente es el fortalecimiento del sistema operativo y de las diferentes aplicaciones que se usan en el host. Para fortalecer el host debemos considerar lo siguiente:

⁸ <http://www.magazcitum.com.mx/?p=2109#.V5wBkfnhCM8>

Roles de usuarios y funciones: se debe tener en claro que a nivel de seguridad no se puede estar creando usuarios a cada momento que uno necesite. Hay que llevar un control de usuarios para designar que usuario en específico va administrar cada equipo o algún servicio en especial.

Para un correcto Hardening se debe realizar lo siguiente:

- Deshabilitar usuario root
- Solo permitir usuarios específicos para el sistema operativo y para los diferentes servicios a utilizar.

Manejo de contraseñas: plantear un correcto manejo de contraseñas para cada uno de los usuarios creados mediante:

- Restricción a los usuarios que utilicen contraseñas antiguas.
- Tiempo de expiración de contraseñas
- Forzar a los usuarios el uso de contraseñas robustas.

Actualizaciones instaladas: las actualizaciones son muy importantes ya que pueden corregir errores y traer nuevas características que ayudaran a reforzar el sistema operativo.

Bitácora de auditorías: llevar un registro detallado por cierto periodos para ir encontrando, corrigiendo y ver si se están cumpliendo con las medidas de seguridad aplicadas.

Aplicaciones: llevar un control de que aplicaciones se deben instalar y que sean necesarias.

Fortalecimiento a nivel de servicios de red

Se refiere a los servicios que tienen acceso a la red interna y se protege a nivel de:

Sistemas de seguridad: para la protección del sistema se debe implementar sistemas de seguridad, uno de los más conocidos el Firewall. El Firewall impide el acceso no autorizado desde la red externa (Internet) a nuestra red interna, en si el firewall monitorea el tráfico que entra y sale, luego decide si ese tráfico lo permite o lo bloquea mediante reglas especificadas.

Configuraciones de seguridad de servicios y protocolos: al activar cualquier servicio también deberán tener seguridad por ejemplo cifrado en las comunicaciones, usuarios específicos para cada servicio entre otros.

Fortalecimiento a nivel de perímetro

- Son los flujos de entrada y salida de un equipo. Pueden ser:
- Segmentación de la red
- Monitorear el tráfico que entra y sale del equipo
- Implementación de equipos de seguridad (Firewall, WAF, IPS)

IV .- CAUSAS Y CONSECUENCIAS

Es preciso identificar diversas variables para poder determinar cuáles son las causas que conllevan a que existan medidas de seguridad para proteger un determinado bien informático. Es decir, básicamente hay que identificar el valor de bien para poder determinar cuáles son los causales que desencadenarán un conjunto de medidas de seguridad que podrán ser aplicadas a dicho bien, ya que el principal motivo para aplicar medidas de seguridad es que exista algún tipo de impacto o desencadene un conjunto de dificultades que puedan comprometer algún tipo de actividad. Planteando un ejemplo podríamos poner al servidor web como un activo de la organización en donde radica la página web que el usuario final espera poder obtener para realizar, por ejemplo, la consulta sobre su progreso de capacitación, consultar sus consultas médicas, y entre otras actividades, las cuales, se han convertido en hábitos para el usuario final. Aquí es donde radican las causas de un ataque informático, es decir, básicamente quién pretende tomar posesión de un activo, plagiar información de él o simplemente dejarlo inaccesible, son diversos los escenarios en realidad, pero, básicamente el enfoque es en el nivel de

impacto que dicho activo causa dentro de una organización determinada; por ejemplo, el dejar inaccesible un servidor web o la página web que un usuario final busca realizar determinada actividad y que no pueda hacerlo, hace que cause malestar al usuario, el cual a su vez, procederá a levantar una queja a la entidad responsable de dicha página, podría causar que dicho usuario no pueda realizar su actividad cotidiana, alargando o afectando así a otras actividades las cuales dependían de aquella que no pudo lograr, entre otros; del lado de la organización esta puede causar que existan pérdidas monetarias al no poder realizar transacciones durante tiempos prolongados en la página, decremento de ingresos, posibles dependencias internas de la página para atención al usuario, entre otras problemáticas que podrían desencadenarse internamente por solo hecho de que la página web no sea exequible. En conclusión, las causas pueden ser diversas y las consecuencias aún más, pero siempre habrá un análisis en donde se evalúe en base a las posibilidades de que dicho activo sea comprometido, el valor que proporciona a la organización e inclusive las posibilidades de recuperación posterior a un desastre. La motivación principal de un Atacante informático es el daño, el lucro o en general la búsqueda de algún beneficio propio o de algún tercero; por otro lado, las consecuencias, son directamente para la organización la cual no tome medidas de contingencia, políticas de seguridad, toma de acciones legales frente a la situación apegado a las leyes locales vigentes y reglamentos internos de la organización.

V.-SUSTENTO LEGAL

ACUERDO NO. 166 DEL 19 DE SEPTIEMBRE DE 2013

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

Artículo 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Artículo 2. - Las entidades de la Administración Pública implementarán en un plazo de dieciocho (18) meses el Esquema Gubernamental de Seguridad de la Información (EGSI), que se adjunta a este acuerdo, a excepción de las disposiciones o normas marcadas

como prioritarias en dicho esquema, las cuales se implementarán en (6) meses desde la emisión del presente Acuerdo.

Artículo 3.- Las entidades designarán, al interior de su institución, un Comité de Seguridad de la Información liderado con un Oficial de Seguridad de la Información, conforme lo establece el EGSi y cuya designación deberá ser comunicada a la Secretaría Nacional de la Administración Pública, en el transcurso de treinta (30) días posteriores a la emisión del presente Acuerdo.

Artículo 5.- La Secretaría Nacional de la Administración Pública realizará de forma ordinaria una revisión anual del EGSi en conformidad a las modificaciones de la norma INEN ISO/IEC 27002 que se generen y de forma extraordinaria o periódica cuando las circunstancias así lo ameriten, además definirá los procedimientos o metodologías para su actualización, implementación, seguimiento y control

Artículo 6.- Es responsabilidad de la máxima autoridad de cada entidad mantener la documentación de la implementación del EGSi debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

Art. 4.- Propiedad Intelectual. - Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Art. 5.- Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 8.- Conservación de los mensajes de datos. - Toda información sometida a esta Ley, podrá ser conservada; éste requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

- Que la información que contenga sea accesible para su posterior consulta;
- Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
- Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
- Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

Art. 48.- Consentimiento para aceptar mensajes de datos. - Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

DE LAS INFRACCIONES INFORMÁTICAS

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos enumerados:

"Art. ...- El que, empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida

en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

VI.- CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

Mediante el presente análisis podemos concluir que las Instituciones Gubernamentales deben tener un alto grado de seguridad a nivel de las aplicaciones informáticas que manejan, ya que las mismas contienen información confidencial de los ciudadanos que acuden a ellas para realizar algún trámite o proceso respectivo.

Además, concluimos que la seguridad informática es uno de los puntos que son dejados en un último plano al momento de desarrollar aplicaciones, lo que no es muy recomendable debido a que éstos vacíos a nivel de seguridad pueden ser explotados por personas malintencionadas que podrían poner en riesgo la estabilidad del aplicativo u obtener información delicada que en manos equivocadas podrían ser un riesgo muy alto para la institución gubernamental.

Tener vulnerabilidades en aplicaciones web o aplicaciones móviles hacen que sean fácilmente atacadas y pueden provocar la pérdida de información importante, en los cuales pueden resultar perjudicados tanto las Instituciones Gubernamentales como las personas que acuden a las mismas, ya que se pone en riesgo la disponibilidad de las aplicaciones como también los datos o información que son almacenados en los mismos.

Finalmente, podemos indicar que la seguridad es un campo muy amplio y en crecimiento, que se debe brindar la mayor atención posible, ya que existen cada vez más personas

malintencionadas que intentan obtener datos o acceso a sistemas vinculados o propios de Instituciones Gubernamentales para indisponer los servicios u obtener información confidencial.

RECOMENDACIONES:

Como recomendación principal se indica que se debe prestar mayor atención a la aplicación de metodologías y normas que permitan fortalecer la seguridad informática para garantizar que la Confidencialidad, Disponibilidad e Integridad de los aplicativos que se están utilizando para de ésta manera obtener como resultado,

aplicativos que tengan un bajo grado de vulnerabilidad en los aplicativos.

Apegarse a la reglamentación y leyes vigentes a momento de aplicar la seguridad en las aplicaciones para de ésta manera no violar las leyes y que esto conlleve a inconvenientes legales que puedan representar problemas a la Institución Gubernamental o a los Ciudadanos que acuden ella.

Finalmente, se recomienda que Institución Gubernamental elabore mecanismos internos y externos que controlen el acceso de personas a los diferentes módulos de los aplicativos mediante la correspondiente segmentación de usuarios y de clientes que vayan a hacer uso de los diferentes aplicativos web y aplicativos móviles para de ésta manera tener mayor seguridad en el acceso a los mismos.

BIBLIOGRAFÍA

LIBROS

López, P. A. (2010). Seguridad informática. Madrid: Editex

Alegre Ramos, M. D., & García-Cervigon Hurtado, A. (2011). Seguridad Informatica. Madrid, España.

TESIS

Jiménez, M. J. (2014). Políticas de seguridad informática en el departamento de tecnologías de la información y comunicación en beneficio de la universidad técnica estatal de Quevedo. Manual de procedimientos 2014. Quevedo. Retrieved from <http://repositorio.uteq.edu.ec/bitstream/43000/130/1/T-UTEQ-0010.pdf>

GrupoSG. (2016). Informe Técnico Proyecto CNE, para Consejo Nacional Electoral; Desarrollado en la Facultad de Matemáticas y Físicas de la Universidad de Guayaquil. Guayaquil - Ecuador: Ciclo 1, Ingrid Elizabeth Espinoza Robles, Vicente Alexander Cevallos Cedeño, Melissa Nathali Andrade Ureta, José Luis Bonilla Lastra, Jefferson Antonio Montes Briones.

REVISTAS

Sánchez, E. P. (6 de Marzo de 2013). Hardening. (editorial@magazcitum.com.mx, Ed.) Magazcitum. Obtenido de <http://www.magazcitum.com.mx/?p=2109#.V5wBkfnhCM8>

Karla Maribel Ortiz Chimbo, José Medina Moreira, Jennifer Alexandra Astudillo Galarza y Kenys Elizabeth Holguín Quijije (2016): "El uso de las nuevas tecnologías al servicio del buen vivir y las gestiones administrativas del servicio público", Revista Contribuciones a las Ciencias Sociales, (enero-marzo 2016). En línea:
<http://www.eumed.net/rev/cccss/2016/02/servicios.html>
<http://hdl.handle.net/20.500.11763/CCCSS-2016-02-servicios>

SITIOS WEB

Mieres, J. (2009). Ataques informáticos. Retrieved from https://www.evilfingers.com/publications/white_AR/01_Atques_informaticos.pdf