EL DESARROLLO DE UN SOFTWARE SEGURO LA MEJOR OPCIÓN PARA PROTEGER LA INFORMACIÓN

ANWARD ARMANDO ACOSTA PIÑEROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA,
BAHÍA MÁLAGA – VALLE DEL CAUCA, COLOMBIA
2020

EL DESARROLLO DE UN SOFTWARE SEGURO LA MEJOR OPCIÓN PARA PROTEGER LA INFORMACIÓN

ANWARD ARMANDO ACOSTA PIÑEROS

MONOGRAFÍA DE GRADO PARA AL OPTAR TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

ESP. EDGAR MAURICIO LÓPEZ ROJAS
DIRECTOR DEL PROYECTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA,
BAHÍA MÁLAGA – VALLE DEL CAUCA, COLOMBIA
2018

Nota de aceptación

_____
_____
_____
_____

_____
Decano de Facultad

_____
Director Trabajo de Grado

_____
Jurado

_____
Jurado

Málaga Buenaventura, 16 de diciembre del 2018.

DEDICATORIA

A mi madre, por su eterna compañía y apoyo para luchar por mis metas y sueños. A mi familia por ser el apoyo incondicional en todo lo que quiero hacer.

Anward Acosta Piñeros

AGRADECIMIENTOS

Anward Armando Acosta Piñeros expresa su agradecimiento a:

Primeramente, a Dios por concederme la oportunidad de seguir avanzando en mi desarrollo como profesional, a su vez por darme el esfuerzo, la voluntad y el conocimiento adecuado para poder trazar el camino que me llevará a cumplir la gran meta personal y profesional.

A mi familia, que siempre han estado con su apoyo y colaboración incondicional logrando así una gran ayuda, en los diversos momentos donde creí desfallecer, donde las ideas no fluían, donde no sabía por dónde avanzar y que por medio de ellos lograba encontrar las ideas necesarias para continuar con el desarrollo de esta monografía. Ellos siempre serán para mí el motor de mi vida, para continuar a diario con mis metas y logrando así estar presentes siempre en cada momento y en cada logro de mi vida.

Gracias a mi persona, por saber que se puede avanzar cuando hay disposición para hacerlo y todo se puede lograr después que exista la dedicación.

CONTENIDO

pág.

LISTA DE FIGURAS

GLOSARIO

Activo (Asset)

Es un proceso, técnica, que posee un beneficio de estructuración, estos activos pueden ser: maquinaria y equipamientos, incluso los archivos y la documentación.

Adware

Software gratis que exponen anuncios, avisos de instalación o adquisición, habitualmente el diseñador recauda por los anuncios que se observan, el anuncio se evidencia en el momento que el software es instalado en el equipo.

Antivirus

Es un Software creado para la identificación, preparación y ejecución del Software defectuoso o perjudicial para la organización.

Ataque de Fuerza Bruta

Modelo de ofensiva que busca que el asaltante intente en todas las maneras admisibles una conexión de vocablo, dígitos y modo existente para descifrar la clave o PIN.

Inspección

Es una intervención neutral a una labor o procedimiento dentro una organización, entidad u otros organismos.

Autenticación

Es el método de comprobar la autenticidad que se le exige al individuo a través de una verificación como método de registro de entrada.

Licencia

Es la fase de concretar la franquicia o autorizaciones respectivas a la persona (estipula la jurisdicción y no puede producir).

Descenso de Voltaje (Brownout)

Sucede cuando el voltaje baja de modo seguido desde un punto de fuente electrónico.

Biometría

Son estrategias que se utilizan para la autenticación o identificación de un sujeto. Los modelos más utilizados en la biometría se encuentran: escaneo de marcas dactilar, patrones faciales, venas de las manos o geometría de la palma de la mano.

Acta Digitalizada

Documento que consta la autenticación de un cifrado público.

Traducir

Es el método de transformación de un escrito claro a uno cifrado.

Cifrar

Escribir un mensaje un texto en clave mediante un sistema de signos formados por número, letras y símbolos.

Confidencialidad

Es la que garantiza la protección de los datos que puedan ser accesibles únicamente al personal autorizado.

Controles Detectivos

Son todos aquellos controles creados para la detección o aparición de algún riesgo, error o acto deliberado dando su reformulación o solución.

Controles Disuasivos

Son los que reducen la probabilidad de un ataque delibrado.

Criptoanálisis

Es el estudio de estrategias para alcanzar a encontrar las debilidades de un sistema con el fin de burlar la seguridad sin tener en cuenta sus respectivos datos.

Criptografía

Es la estrategia de transformar el mensaje el cual sea accesible por medio de claves que únicamente el emisor y destinatario saben.

Criptología

Disciplina que se dedica al estudio de la escritura secreta en mensajes, de tal manera sean complicados de ejecutar por entes facilitando su acceso.

DDoS (Ataque distribuido de negación de Servicios)

Ataque multiple a los servidores desde varias computadoras para detener su debido funcionamiento.

Defensa en profundidad (o en capas)

Prototipo que defiende y procura adaptar dominio e inmunidad para resguardar toda la información en capas desiguales. La estrategia es lograr que impostor obtenga la información que necesite.

Descifrado

Aclarar el significado de la información oculto en un mensaje en códigos o codificado.

Disponibilidad

Es la transformación de garantizar los datos, información sean alcanzables a los beneficiarios permitidos en el momento que se necesite.

Due Care (Cuidado Necesario)

Son todos los movimientos necesarios a realizar para la protección de los intereses del usuario final.

Due Diligence (Diligencia Debida)

Son las practicas de las actividades debidas que buscan mantener el esfuerzo realizado por el Due Care.

Dumpster Diving (Buceo de Contenedores)

Es la búsqueda de información en la basura o desechos de la victima con la pretensión de buscar puntos vulnerables para un ataque.

Espionaje

Practica y conjunto de técnicas asociadas a la obtención de datos o información clasificada.

Corta fuegos (firewall)

Software o Hardware de la estructura informática que es implementada para crear controles de ingreso o salidas permitidas o no permitidas, con el fin de aislar contenido considerado peligrosos.

Forense (Informática Forense)

Es la disciplina que se encarga de obtener, identificar, analizar, preservar, mediante técnicas científicas y analíticas, con el fin de presentarlos en un proceso legal.

Función Hash

Una función aritmética que diseña un gráfico único de conjuntos considerantes de información. La operación Hash se utiliza seguidamente en algoritmos criptográficos, para realizar recapitulación de avisos (Checksums and message digest).

Gateway (puerta de enlace)

Estructura informática configurada para interactuar como interfaz de conexión entre dispositivos informáticos, el cual permite compartir entre estos.

Honeypot

Es una herramienta que se utiliza en la informática para la protección y especialmente se basa en absorber y estudiar ataques de Bots y Hackers.

Identificación

Es la capacidad y manera adecuada de identificar de forma exclusiva a un usuario dentro de un sistema, asi mismo es la forma de demostrar que el usuario que ingresa es la persona que es.

Integridad

Respalda la precisión y complejidad de los datos en la manera de que su método para el procesamiento sea el adecuado.

Negación de Servicios (DoS)

Es una arremetida a la red o servidor con la determinación de producir que la estructura no esté utilizable.

Propiedad Intelectual

Posibilita al inventor o propietario de un título, lema, obra a gozar de beneficios de las inversiones realizadas en la realización de una obra o diseño.

Pruebas de Caja Negra

El sujeto realiza el ensayo de seguridad sin tener algún tipo de estudio preciso de la estructura que se está colocando a evaluar.

Texto Cifrado (Hipertexto)

Todo mensaje codificado que transmite información, pero no es legible a menos que se descifre, la seguridad del texto depende de usar un cifrado seguro y mantener la clave en secreto.

RESUMEN

Hoy en día la tecnología es un componente necesario para cualquier estructura sin importar el sector, siendo la encargada de emplear de una manera apropiada la seguridad digital, diseñando normas, técnicas y procedimientos, logrando mantener condiciones seguras durante el procesamiento de datos. Debido a esto se debe tener en cuenta tomar las determinaciones y órdenes (necesarias) ineludibles en cualquier sitio laboral previamente se pueda provocar un suceso de infalibilidad de los datos, como lo sería una fuga de la misma.

La infalibilidad de los datos se vincula referentemente a tres evaluaciones, las cuales son el apoyo referente de adaptar los espacios de seguridad de nuestros respectivos datos.

- Los recursos de los datos que están anteriormente se vinculan a la asesoría para que esté asequible en el momento que sea necesaria. En ciertos prototipos se carece de estos recursos para la indagación como lo son: en el tiempo que nos sea difícil el acceso al correo electrónico siendo necesario a una inexactitud de distribución o provechoso, en el momento que se lleva una ofensiva de denegación de servicio, en cual la estructura "cae" o imposibilita el acceso a entradas genuinas. Al suceder esto ambos tendrían intervención formal para la protección de los datos.

- La privacidad involucra que el dato sea alcanzado o accedido exclusivamente por la persona a la cual se le dio su respectiva autorización en el intervalo establecido, con el fin que el respectivo dato pueda ser accedido únicamente por aquellos individuos, empresas o estructuras sistematizadas las cuales están autorizadas para su ingreso. Se debe apreciar que la aceptación de una designada inspección para enriquecer la protección, es perjudicar de aspecto negativo o positivo para la evaluación, debido a esto, es muy importante distinguir cuál de estas evaluaciones son esenciales para la seguridad. Por ejemplo, introducir un proceso de entrada para resguardar la privacidad en una estancia de procedimientos, conseguirá ocasionar un aplazamiento en la entrada de los datos perjudicando su disponibilidad.[1]

El problema en investigación de esta monografía se manifiesta a través del siguiente planteamiento.

[1] https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

¿Cuál es el interés en la protección informática y como a través de la metodología Security Requirements Engineering Process se puede proteger la información?

En este sentido, podrá dar a la sociedad una idea clara de la necesidad y de todo lo que respecta a beneficios de esta investigación la cual tiene como objetivo fundamental, describir como a través de la metodología Security Requirements Engineering Process nos permita proteger la información.

Palabras clave: SEGURIDAD, HERRAMIENTAS, SISTEMA OPERATIVO, SO, LINUX, WINDOWS, MAC, ESTRATEGIA, HARDENING, INSTALACIÓN, MÉTODOS, MONITOREO, INFORMACIÓN, APLICACIÓN, ANTIVIRUS, TRANSACCIONES.

ABSTRACT

Today technology is a necessary component for any structure regardless of the sector, being responsible for using digital security in an appropriate way, designing standards, techniques and procedures, managing to maintain safe conditions during data processing. Due to this, it is necessary to take into account the unavoidable (necessary) determinations and orders in any work place, an infallibility event of the data can be provoked, as it would be a leak of the same.

The infallibility of the data is linked referentially to three evaluations, which are the reference support for adapting the security spaces of our respective data.

❖ The data resources that are previously linked to the advice so that it is affordable at the time it is needed. In certain prototypes these resources are lacking for the investigation as they are: in the time that it is difficult for us to access the email being necessary to an inaccuracy of distribution or profitable, at the moment that an offensive of denial of service is carried out, in which the structure "falls" or prevents access to genuine entries. When this happens, both would have formal intervention for data protection.

❖ Privacy implies that the data is reached or exclusively by the person to whom their respective authorization was given in the established interval, so that the respective data can be only by those individuals, companies or systematized structures which They are authorized for admission. It should be appreciated that the acceptance of a designated inspection to enrich the protection is to damage the negative or positive aspect of the evaluation, because of this, it is very important to distinguish which of these evaluations are essential for safety. For example, introducing an entry process to protect privacy in a stay of procedures, will result in a postponement of the entry of data damaging its availability.

The research problem of this monograph is manifested through the following approach.

What is the interest in computer protection and how can the information be protected through the Security Requirements Engineering Process methodology?

In this sense, you can give society a clear idea of the need and everything that concerns the benefits of this research, which has as its main objective, to describe how, through the Security Requirements Engineering Process methodology, we can protect the information.

Key Words. SECURITY, TOOLS, OPERATING SYSTEM, SO, LINUX, WINDOWS, MAC, STRATEGY, HARDENING, INSTALLATION, METHODS, MONITORING, INFORMATION, APPLICATION, ANTIVIRUS, TRANSACTIONS.

INTRODUCCIÓN

En informática la seguridad informática o ciberseguridad es la técnica o área la cual se enfoca en la búsqueda de mecanismos o creación de programas, para la protección de la información que circule en una red, ya sea local, empresarial o continental, logrando así las distintas complacencias y exigencias fundamentales anheladas por la humanidad, las cuales se puedan dar en el desarrollo del entorno o mecanismo.

Se debe tener en cuenta con dicha definición que desde sus orígenes la ciencia por medio de la tecnología ha venido siendo utilizada para saciar los requisitos primordiales (comodidades cotidianas y entorno social y cultural), en la actualidad para satisfacer sus necesidades físicas y estéticas (acciones deportivas, vanidad y hobbies) para saciar deseos personales (estatus social, producción de todo tipo armamento y todo aquello que ayude al dominio de la humanidad).

Cabe resaltar que la ciencia trae considerables utilidades a la humanidad ya que dentro su estrategia primordial está diseñar buenos mecanismos provechosos para facilitar su duración e impulso. Desde todo punto de vista observamos que la ciencia arriesga una función importante para el entorno social porque afortunadamente se puede facilitar un dialogo de manera rápida entre todos como lo es la telefonía celular, intercambio de mensajes, entre otras más.

La función en cuanto a la tecnología influencia en el desarrollo socio-económico de nuestra sociedad, lo cual hace que en la actualidad las redes informáticas se hayan convertido en pilar fundamental para la humanidad, ya que por medio de estas llegamos a compartir toda clase de archivos, video llamadas y demás servicios. Y donde las redes informáticas no poseen barrera alguna y están permitiendo tener contacto con lugares remotos lo que se ha vuelto un elemento necesario en nuestro diario vivir.

Partiendo de la importancia de las comunicaciones existentes en la red, se han optado distintos sistemas de seguridad, con los cuales se pretende garantizar que las llamadas y archivos compartidos solo sean visto, escuchados al destinatario y no a terceras personas, con esto se logra que no se realicen robos, daños de información las cuales están al orden del día de la ciberdelincuencia.

Es por esto que la importancia de este trabajo y que dentro de el mismo se va a dar a conocer a cada una de las personas interesadas de nuestra sociedad los beneficios que podrán encontrar en la metodología Security Requirements Engineering Process, toda vez que por medio de esta obtendrá una mayor seguridad para su compañía, para su micro o macro economía y para su vida personal y profesional dentro de la transmisión de datos u archivos en diferentes plataformas. Trayendo consigo la protección de datos y eliminando la fuga de información, lo cual podrá ser analizado dentro de esta investigación.

1. DEFINICION DEL PROBLEMA

LA SEGURIDAD INFORMÁTICA Y SUS BENEFICIOS EN LA SOCIEDAD.

1.1. PLANTEAMIENTO DEL PROBLEMA

La protección es esencial en las personas que la acción de alguna idea o aspiración existencial. como lo indica el autor Rosales (2002, p.33) Al proponer “La seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella”. Por tal razón se conoce que la convicción en la tecnología en coexistir si se reúnen aquellos instrumentos y estrategias probables ya que algún método empleado por el mismo le es difícil de incluir en cada uno de los puntos delicados de la estructura en la aclaración como indica, Hallberg (2003, p.97).

Cabe resaltar que la confianza depositada en la seguridad informática propone dar el nivel de confianza en las distintas organizaciones, las cuales no logran dar por si mismas una confianza en la protección de la información, es también de conocimiento que la seguridad informática no puede por sí misma con el desarrollo avanzado de los medios tecnológicos en la elaboración de software seguro, donde este es el eje principal de toda empresa para la protección de su información; lo cual hace necesario que se implementen metodologías efectivas para el proceso seguro de software desde los periodos más tempranos de este proceso y que puedan ser implementadas en las distintas etapa: requisitos, diseño, desarrollo y pruebas.

Uno de los principales retos en las estructuras y particularmente en los departamentos de sistema y/o informática es el resguardo de los datos. Esta cuestión es atinar a diferentes prohibiciones en donde el profesional en sistemas opina que sencillamente con el proceso de asentar un instrumento a la altura de hardware o software en un sistema este estará seguro ante un ataque cibernético, a sabiendas que solo con esto no estarán seguros ante un posible ataque que se pueda presentar por los hackers, quienes siempre están en constante búsqueda de victimas para sabotear la información.

“La seguridad usada en cualquier fase de un sistema informático no asegura que este se encuentre fuera de cualquier peligro, daño y/o riesgo que pueda afectar la estructura informática. Se comprende como amenaza o perjuicio íntegramente aquello que daña la actividad directa o el resultado logrado. Para los profesionales del área la concepción de protección en la tecnología es ilusorio por alguna razón negativa el no contar con un sistema 100% protegido. Para que en una estructura se considere eficaz hay que tener presente estas características:

- Integridad: la información sólo puede ser modificada por quien está autorizado.
- Confidencialidad: la información sólo debe ser legible para los autorizados.
- Disponibilidad: debe estar disponible cuando se necesita.
- Irrefutabilidad: (No-Rechazo o No Repudio) que no se puede negar la autoría.

Observando el origen de las amenazas, la inmunidad ayuda a obtener una protección en logística y protección física.

Actualmente la protección de los datos es un tema de alta prioridad ya que es obligatorio en los usuarios de la red para proteger y a su vez su respectiva privacidad no sea violada". Según Jesús Rodea (1994, p.26) "la infalibilidad es un asunto de carácter obligatorio para alguna entidad, si está o no conectada a un sistema de carácter público. Únicamente asimismo se puede observar.

El horizonte o meta de la protección que se emplee, depende hasta donde se desea llegar por parte del beneficiario o usuario final.

La protección en el sistema y archivos es más fácil al tener un FIREWALL. Para plantear un desarrollo en protección es recomendable usar (al menos) estos instrumentos.

- Un FIREWALL o combinación de ellos.
- PROXIES
- Un sistema de detección de intrusos o IDS.
- Sistema de actualización automática de software.
- Sistemas de control de la integridad de los servidores, paquetes, entre otros.
- Un sistema de administración y control para monitorear la seguridad".

Según George Beekman (1996, p.45).

Es necesario analizar que dentro de nuestra rutina diaria se encuentran inmersas actividades donde se requiere el uso obligatorio del internet, manejo de datos por medio del computador, celular y demás medios tecnológicos que podamos tener a disposición diaria. Lo cual nos deja expuestos ante todos los cibernautas y Hackers existentes en el planeta que solo buscan la satisfacción personal de haber cumplido con su objetivo, boicotear todo tipo de información y servicios que se encuentre guardados o alojados en la nube, plataformas, software y/o todo lugar que almacene información. Es por esto que como sociedad debemos hacer frente a este tipo de exposición y llevar a cabo la ejecución de acciones que sean encaminadas a prevenir que este tipo de eventos sucedan dentro de nuestra vida personal, profesional, empresarial, entre otros.

Es por esto que debemos incorporar a nuestro diario vivir el software y las medidas de seguridad personales buscando siempre la manera que estas sean aplicadas a

la información que estamos manejando, lo cual nos permitiría tomar decisiones con respecto a cuál usar para la protección de nuestros datos e información.

Para la sociedad, hoy en día se debe realizar la concientización de la necesidad del uso de software para la protección de sus datos, toda vez que creemos que el simple hecho de usar las redes o demás alternativas que nos genera el internet es seguro, generando así un nivel de confianza en la información que aportamos en las redes.

Es por esto, que se hace necesario hacerle ver al usuario que debe preocuparse porque todo lo que haga y deje de hacer con la tecnología se encuentre respaldado (cuidado).

Teniendo en cuenta lo anterior el presente trabajo monográfico busca establecer los beneficios de la seguridad informática en la sociedad.

1.2. FORMULACIÓN DEL PROBLEMA:

¿En qué se beneficia una sociedad de la protección Informática?

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Desarrollar una indagación que permita establecer la importancia del desarrollo de software seguro mediante la Metodología Security Requirements Engineering Process y cuál es su impacto positivo para la sociedad.

1.3.2 OBJETIVOS ESPECÍFICOS

- Indagar cuáles son los riesgos y amenazas más frecuentes en el progreso del software seguro y como pueden evitarse.

- Establecer cuáles son las etapas del proceder del software seguro que puedan ser implementados para el desarrollo de un programa de software.

- Hacer un análisis de la metodología Security Requirements Engineering Process que permita conocer su funcionalidad y aplicabilidad para el desarrollo de un software seguro.

1.4 JUSTIFICACIÓN

Teniendo en cuenta lo analizado anteriormente cabe ondear en buscar definiciones para el tema de la seguridad y es donde encontramos que la seguridad es un rasgo que debe ser implementado en cualquier infraestructura sea informática o no, el cual nos asegurara que el sistema que se está siendo utilizado está libre y protegido de peligros, daños y que es un software seguro. Como este rasgo, especificando para el Software informático o redes de datos, es muy difícil de obtener según lo que establecen muchos expertos en sus apartes, se toma como aclaración en protección, se puede hablar de confiabilidad; siendo la posibilidad que el sistema actué en una manera segura; por tal razón hace referencia a la estructura confiable en parte de sistemas seguros.

Al tener en cuenta dicha definición es bueno saber que buscamos o queremos proteger y es aquí donde encontramos que los tres componentes principales que corresponden a la seguridad o blindar en la estructura de la información como lo son el software, el hardware y la información. En donde el Hardware es el conglomerado de total de los componentes tangibles o somáticos que posee una estructura de información, las CPU, terminales, medios de almacenamiento (USB, CD, entre otros.). El software es el compuesto de esquemas lógicos que se encargan de hacer funcionar al hardware e interpretan las ordenes emitidas desde el teclado o un mouse, tanto sistemas operativos como aplicaciones, y por ultimo tenemos que la información o datos que son el grupo de los datos que asesora y dirigen el funcionamiento el software y el hardware, como ejemplo tenemos los paquetes de información de origen la cual recorre por una estratagema cableada o la información almacenada. Generalmente en auditorías se consideran que ver con la certeza de que se trata de una habitación componente en proteger, este cuarto componente son los fungibles que son los elementos de uso diario que tienden a sufrir un desgaste con el uso continuo, estos elementos pueden ser, el papel de impresora, tóner, cintas magnéticas, CD, entre otros no se tiene en cuenta la protección este componente por tratarse de agentes externos al sistema, pero siempre hay que tener en cuenta que es lo que se imprime, ya que puede tener información de uso privativo de la empresa.

Dentro de los tres componentes a proteger normalmente son los datos o la información el principal elemento es resguardar, teniendo en cuenta que son los más propensos a subir amenazas en cuanto a la información que se tenga allí, y muy probable los difíciles volver a tener sino se tiene un respaldo de la información: normalmente el servidor o equipo que ejerza estas funciones estará ubicado en un compartimento el cual tiene un acceso restringido y se encontrara en un entorno inspeccionado en un acontecimiento de ausencia de en uso está la cual se ´puede recuperar sin complicaciones estando en su punto de origen. (por ejemplo, el CD-ROM con el sistema operativo que se utilizó para su instalación). Sin bloqueo en algún acontecimiento presentarse una confusión referente a una procedencia de

archivos o plan, no tenemos un medio desde el cual se pueda restaurar: para tratar de recuperar esta información debemos tener obligatoriamente unos controles para la realización de duplicado de protección y esperar que la habilidad de duplicados de seguridad implementada sea muy exacta, esto con el fin de lograr restaurar toda la información comprometida, en caso de no contar estricta estructura de copias de protección es difícil reestablecer los datos al estado en el cual se encontraban antes de la pérdida.

Al tener claridad de que buscamos proteger, debemos ahora ondear en lo que respecta a la amenaza existente dentro del manejo de las tecnologías, las cuales no pueden ser desconocidas por la sociedad porque son el diario vivir de cada uno. Esto permite verificar a ciencia cierta de que nos debemos proteger, es aquí donde con lleva hablar respecto a las siguientes amenazas a la seguridad; humanas donde están las maliciosas (que son externas e internas), las no maliciosas (provienen de empleados ignorantes). También dentro de estas amenazas están las catástrofes naturales como lo son un incendio, las inundaciones y los terremotos.

Ilustración 1

Fuente: autor

Es entonces que en esta investigación se busca establecer a que se refiere cada una de las amenazas establecidas anteriormente para poder saber a qué se está afrontando la sociedad en cada uno de estos puntos.

- Dentro de las amenazas humanas están las maliciosas (las externas e internas), las no maliciosas (empleados ignorantes).

  En general los asaltantes en la estructura de información provienen de individuos que, intencional, desean provocar cuantiosos daños o pérdidas ya sean económicas o de información. Comúnmente se tratará de hackers que intentaran conseguir el privilegio más alto que se tenga en el sistema aprovechando algún bug o falla en la programación del software.

- Personal, normalmente las advertencias existentes para una estructura de informaciones que provienen de los empleados de la empresa son pocas veces tenidas en cuenta; debido a que se presume y existe un ambiente laboral tranquilo, con esto se evidencia que un individuo de la empresa, inclusive distinto al área de sistemas pueda implicar protección la información almacenada en los equipos.

- Ex-empleados, otras personas que siempre estarán probablemente atraídos en asaltar o hacer vulnerable nuestra estructura son los ex-empleados, en especial quienes fueron despedidos o aquellos que se fueron a la competencia. Normalmente estas personas se encuentran descontentas en donde pueden aprovechar las vulnerabilidades que conocen perfectamente del sistema para ingresar y atacarlo con motivo de represarías por alguna eventualidad que no creen que son justificables, aquellos daños que pueden hacer estas personas pasan desde insertar troyanos, virus o únicamente se conectan al sistema para sustraer información, (el que se conecte un ex-empleado a la empresa es un error ya humano en donde no sea desactivado la cuenta de esta persona) logrando con esto dañarlo de la forma que crean justa o llegando incluso a chantajear la entidad en la cual elaboraron.

- Intrusos, en conjunto con los crackers, son asaltantes más comunes que podemos encontrar, estas personas nacen del interés por las nuevas tecnologías, normalmente son estudiantes, los cuales están trabajando en entornos con equipos con pocos privilegios, estos buscan un mayor privilegio de acceso al que tienen y en su colectividad de sus acontecimientos se desarrolla en forma recreativa, como reto personal con el fin de leer el correo de un amigo o poner en evidencia que es admisible saltarse la protección de una red, en la mayoría de veces estos casos se consideran ofensivos mas no destructivos.

- Crackers, los encontramos en los entornos que poseen seguridad media, los cuales son los objetivos normales de estos intrusos, ya que siempre están en búsqueda de fisgonear, con el fin de usarlas como enlace a otras redes. Normalmente estas organizaciones son libres y su protección no suele ser una causa que se tenga presente, ya que al tener una diversidad de estructuras puestas en contacto con estos sistemas ocasiona que tenga vulnerabilidades ya conocidos. De esta manera el atacante sólo debe ejecutar una copia protegida que resista el control y posteriormente proceder a asaltar mediante un exploit a los sistemas que exponen debilidad.

- Terroristas, son aquellos atacantes que ataca al sistema en fin de provocar algunas formas de prejuicio. Un ejemplo puede ser alguien intentando borrar la información contenida en carpetas de direcciones de un grupo administrativo y/o religioso enemigo.

- foráneos pagados, es considerado el grupo de asaltantes más amenazador, ya que pueden ser contratados por una tercera persona o son los que habitualmente atacan a las empresas más grandes de la red, se tratan de atacantes con gran experiencia en la evasión de los distintos filtros y seguridad, los ataques habitualmente están destinados a la obtención de información reservada de la empresa o en casos extremos el secuestro de información en donde se pide un rescate por su liberación, normalmente estos atacantes disponen de todos los medios necesarios para realizar su ataque.

Las siguientes amenazas están enmarcadas como malware, este término podemos decir que se origina de la unión de las palabras (malicious software), este esquema es perjudicial para el sistema, el cual se ha creado para la inserción de virus, gusanos, troyanos, spyware o incluso bots, con las cuales se intenta obtener su blanco, como puede ser la recolección de datos que se obtenga de la víctima, beneficiario o sobre el ordenador en sí,

- Amenazas lógicas: en esta categoría encontramos todo tipo de software que perjudican la toda la estructura digital los cuales fueron diseñados con este fin o inocentemente por error de programación (bugs o agujeros).

- Puertas traseras, Es común que los programadores inserten 'laberintos' en la estructura (código fuente) original de un software, a estas variantes se les conoce como salidas finales y con esto se obtiene una mejor escalamiento al momento de identificar y perfeccionar los defectos encontrados en el sistema, un ejemplo, es cuando los creadores de un software de administración determinan el poder ingresar a una determinada lista se necesitaran cuatro claves distintas con ciertas características, el programador puede realizar una rutina en donde podrá obtener ese ingreso a través de una sola contraseña con el propósito de no desaprovechar su periodo al depurar la estructura del software.

- Bombas lógicas, son fragmentos de código dentro del software o sistema que se perpetua sin efectuar alguna actividad hasta que sean accionadas en forma local o remota, cuando son activadas la función que realizan van en contra de la función original en donde se trata de una acción perjudicial. La forma de activación más común es la llegada de una fecha concreta.

- Virus: es una serie de código que es insertado en un documento el cual es manejable de manera que pueda ser ejecutado, al activarse un virus es capaz de replicarse a sí mismo en otros archivos.

- Gusanos: es un programa que tiene la capacidad de ejecutarse y propagarse a voluntad propia a través de redes, este tipo de programa permite mecanizar y actuar en un corto tiempo el total de los procesos que normalmente efectuaría un asaltante normal para ingresar a la estructura, normalmente el gusano tardaría unos pocos minutos para controlar una red completa, cosa que no sucede con una persona, que podría tardar horas en controlar la red.

- Caballos de Troya: también conocidos como troyanos son directrices alojadas y ocultas en un archivo de tal manera que luce que se estuviera realizando una acción legitima por el usuario, no obstante, verdaderamente está realizando actividades escondidas a la vista del beneficiario.

- Spyware: se encarga de recopilar datos sin el conocimiento o consentimiento de la víctima. Su función más común es recolectar datos de la víctima y entregarlo a entidades o compañías que la deseen, estas aplicaciones son usadas de forma legal para la recopilación de información contra sospechosos de algún delito y así tener evidencias en contra de él.

- Spoofing: es la forma en donde un atacante, se hace pasar por la victima falsificando los datos con intenciones y acciones peligrosa.

- Phishing: es una mezcla de spoofing e ingeniería social, en donde su mayor característica es el adquirir información confidencial de distintas formas fraudulentas, como lo es una contraseña, la información de tarjetas de crédito o información bancaria.

- Spam: son mensajes enviados con información publicitaria que no han sido solicitados, estos mensajes se envían en forma masiva.

- Exploits: Es una técnica que aprovecha la debilidad en protección en la organización de datos con la intención de obtener un mal funcionamiento del mismo, un ejemplo de un mal funcionamiento es el acceso de forma no autorizada al atacante.

Por ultimo podemos entrar a mencionar todas aquellas amenazas lógicas que se pueden llevar a cabo para violentar la seguridad. Entre ellas tenemos las siguientes;

- Mecanismo de infalibilidad: todo mecanismo de protección simboliza un arma de doble filo: así como un administrador emplea estas herramientas usadas para la detección y dar solución a defectos en los datos o subred que administra, el atacante puede utilizarlas para encontrar y manifestar estos errores y así aprovechar para la realización de un ataque a los equipos. Como ejemplos de estas herramientas encontramos NESSUS, SAINT o SATAN las cuales acontece de provechosos a ser riesgoso en el tiempo que

son utilizadas por personas que buscan las vulnerabilidades de una red completa con fines delictivos.

- Técnicas salami: Esta técnica es conocido por el desfalco automático de pequeñas sumas de dinero de una cuenta la cual posee una gran cantidad, esta técnica es efectiva por que la pequeña parte robada hace extremadamente difícil su detección, si esta se realiza y se automatiza para aplicar pequeños descuentos de nóminas, pagos, entre otros, podría llegar a una gran cantidad.

- Amenazas Físicas: las catástrofes manipuladas por el individuo son las amenazas con menos probabilidad de atacar un sistema, ya que siempre se toma en cuenta la ubicación en donde va a funcionar el sistema con el fin de mitigar este tipo de catástrofes.

Ahora bien, conociendo las definiciones de seguridad, las amenazas que nos rodean, y la detección de quienes son de los que nos debemos defender, cabe aclarar ahora el cómo debemos hacer para defendernos de dichas amenazas. Es aquí donde obtenemos que las seguridades se dividen en tres grandes mecanismos de defensas como lo son: los de prevención, los de detección y los encargados de la recuperación. En los mecanismos de prevención encontramos que son los que se encargan aumentar la protección de la estructura mientras realizan sus actividades normales, logrando así la prevención de la violación a la seguridad, un ejemplo claro de estos, es el cifrado que se aplica a la transmisión de información, ya que con esto evita que un atacante escuche, lea, la información que se transmite.

Los mecanismos de detección son aquellos utilizados en la detección de la violación a la seguridad o en los intentos fallidos de violación; un ejemplo de este mecanismo son los programas usados en la auditoria. Entonces y según lo anterior cabe decir que los dispositivos de restauración son los que se adhieren en el tiempo a la violación en la organización ha sido detectada o en el peor de los casos logro borrar, modificar la información contenida, este mecanismo se usa con el fin de su funcionamiento correcto, dentro de los ejemplos del mecanismo de recuperación están el uso de duplicado de infalibilidad. Así mismo entre el último conjunto podemos encontrar un subconjunto el cual se le denomina como mecanismos de análisis forense, en donde sus objetivos son el de determinar el alcance de la intrusión, las actividades que realizo el atacante en el sistema, y los medios que uso para ingresar, con el fin de prevenir futuras intrusiones en los demás sistemas de nuestra red.

Los mecanismos más usados en la prevención de ataques son articulaciones de verificación e identidad, de verificar el ingreso, de descentralización, de seguridad en las comunicaciones.

Teniendo en cuenta la argumentación anterior se puede concluir que es importante el desarrollo del siguiente trabajo, toda vez que la protección tecnológica es una disciplina que debe velar por la seguridad, la integridad y la privacidad de los datos que se encuentra almacenada en un sistema información. Es por esto, el interés que los individuos posean instrucción ante que se enfrenta cuando decide hacer uso de la tecnología, hacia donde está tomando rumbo su información y que tipo de manejo le está dando a la misma y entre otras situaciones que acontecen en el diario vivir.

Es por esto que la implementación de un sistema de protección a la información nos hace referencia a colocar controles para protegernos de posibles fraudes y bloquear el acceso a personas ajenas al sistema; lo cual nos lleva a pretender proteger la información de ataques externos, por tal razón las organizaciones siempre han invertido todos sus esfuerzos en implementar el área de seguridad informática para proteger a la organización, por lo cual nosotros en nuestras vidas debemos buscar los conocimientos necesarios para que nuestra información no divague en la red, ya que esta información es parte esencial y debe ser tomada en cuenta como un activo más de la organización o nuestra y que de llegarse a perder y/o modificar es difícil de recuperar. Con el avance de la tecnología, los programas sistemáticos y el uso del internet en los últimos años han permitido que la información almacenada en los medios informáticos se haya visto expuesta a continuos ataques de personas inescrupulosas “ciberdelincuentes”.

Es por esto que se hace necesario dar a conocer a la sociedad como a través de la implementación de las metodologías de desarrollo seguro durante las etapas del desarrollo del software nos ayudara y brindara una seguridad temprana: estas etapas van desde los requisitos, la creación, desarrollo y pruebas del software.

Siempre se debe tener presente la seguridad en el sistema desde las primeras etapas de desarrollo y no pasarla a un segundo plano. Además, hace necesario que cada persona se encargue de investigar el desarrollo de aplicaciones seguras con el fin de escoger las metodologías que se adecuen a las necesidades de la aplicación y los requerimientos solicitados por el usuario final. Todo esto le ayudara a la sociedad a usar de manera segura sus datos dentro de la aplicación de la tecnología, que por medio del desarrollo de este importante trabajo se le puede detallar aún más en la temática de su aplicación para hacer de su vida una tranquilidad al momento de entrar en la ola de la tecnología.

Al hablar sobre las distintas vulnerabilidades que se pueden dar o existir en el entorno laboral y en el desarrollo del software, podemos hablar del reporte realizado por welivesecurity filial de la empresa Eset, líder y dueña del antivirus NOD32, donde habla sobre el Máximo histórico de vulnerabilidades que ocurrieron durante el año 2017, se evidencia que los fallas en lo que concierne a seguridad informática aumentaron, llegando a sobrepasar registros históricos de años anteriores llegando a un aumento por encima del 120%, con este incremento se evidencia que

diariamente se reportaban 40 vulnerabilidades a diario, comparando el año anterior que en promedio fueron 17 vulnerabilidades reportadas.

Ilustración 2

Fuente: https://www.welivesecurity.com/la-es/2018/01/04/maximo-historico-vulnerabilidades-2017/

1.5. ALCANCE Y LIMITACIONES

1.5.1. Alcance.

El siguiente estudio se localiza dentro de los planes de investigación descriptiva y lo que pretende esta investigación es lograr la sensibilización a los expertos en la asesoría, acerca de la transcendencia de conocer los beneficios sociales que puede traer la aplicación de la Seguridad Informática en su diario vivir, sus objetivos, fines y alcance, donde a través de ella se encontrarán evidencias que pueden llevar a un siniestro informático dentro de sus labores personales, profesionales, empresariales, entre otras más.

- Primero se revisarán las vulnerabilidades existentes en el sector informático y las técnicas existentes de ataque que utilizan personas inescrupulosas con el fin de cometer actos ilícitos.

- Segunda parte se enfoca en el desarrollo del marco teórico de este trabajo.

- Tercero, se describe el marco legal que debe tenerse en cuenta en el momento al realizar un trabajo de seguridad informática.

- En cuarto lugar, se realiza el desarrollo de la investigación sobre la seguridad Informática y sus beneficios en la sociedad a través de su aplicación.

- Por último, se dan a conocer las conclusiones y recomendaciones pertinentes.

1.5.2. Limitaciones

Durante el proceso investigativo se presentaron las siguientes limitaciones: Restricciones por la ausencia de inspección de ingreso a los datos que se necesitan de los parámetros particulares de uso de la aplicación o preestablecidos por el administrador del sistema, en este caso del margen a analizar socialmente, lo que imposibilitó conocer con exactitud los problemas informáticos que se presentarían en dicho núcleo social.

El tamaño de la muestra analizar para concluir al respecto de los beneficios que aplica en la sociedad el uso de la metodología Security Requirements Engineering Process, se hace muy grande, lo cual nos amplia una investigación muy abierta. Es por esto que nos lleva a tener que buscar métodos de delimitación de la sociedad a analizar que permita obtener una muestra global con resultados reales.

Para subsanar dichas situaciones se realiza una extrapolación de los resultados, para ampliar un poco el margen social a analizar para obtener un mejor resultado

de los beneficios que brinda el uso de la seguridad informática por medio de la metodología Security Requirements Engineering Process.

Es necesario destacar que durante el desarrollo del presente estudio no se llevara a cabo encuesta o algún tipo de voz a voz para obtener información al respecto de que tan confiados se sienten las personas de nuestra sociedad con el uso de las TIC, con el fin de determinar si saben hacia donde van cada uno de los datos que proporciona dentro de la red. Esto no se hará toda vez que será un producto final para concientizar de la importancia del uso, lo cual lleva a establecer la necesidad en la persona que lea el documento de querer usar la metodología Security Requirements Engineering Process en su vida diaria, personal, profesional, laboral, empresarial, entre otras más.

2. MARCO REFERENCIAL

Para la ejecución de este trabajo investigativo es necesario conocer los conceptos más importantes a tratar y que sean concernientes con el tema, es importante contar con el soporte teórico del tema a tratar que admita depurar definiciones con el fin de suministrar respuestas a las exigencias del proyecto; con lo cual cada paso a desarrollar que busca es dar respuesta a los objetivos propuestos.

2.1 SEGURIDAD INFORMÁTICA

La Seguridad son aquellos métodos, estrategias y/o funciones las cuales están determinadas a preparar, proteger y amparar lo que es calificado malicioso, saqueo, extravió o perjuicio, la seguridad comprende diversas dimensiones al enlazar con las estructuras de datos.

Acá podemos encontrar zonas que van desde la seguridad física como lo son los componentes del hardware, lo relacionado con el entorno, hasta la protección de la información contenida en este o las redes que permiten su comunicación con otros sistemas.

Sin embargo, dentro de diferentes autores se puede encontrar un planteamiento como lo es el {Decreto-Ley No. 199} ,[2] que trata al respecto de definiciones tales como "*Seguridad Informática es un conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las tecnologías de información*".

Otra de las definiciones encontradas están la de {Todos@cicese, 2002} , "*Seguridad Informática es el conjunto de recursos (métodos, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo e información, disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo*".

{AUDITORIASISTEMAS, 2004} , exponen "*la Seguridad Informática es el conjunto de reglas, planes y acciones que permiten asegurar la información contenida en un sistema computación*.

[2]http://www.tic.siteal.iipe.unesco.org/normativa/1436/decreto-ley-no-199-nov99-sobre-la-seguridad-y-proteccion-de-la-informacion-estatal

2.1.1 ¿CÓMO PODEMOS PROTEGER EL SISTEMA INFORMÁTICO?

Indicando {BADOPI, 2003} , para tener un buen sistema de protección frente la ofensiva debemos tener presente tres factores principales: la prevención, la recuperación y la detección.

Para empezar, es esencial efectuar un estudio sobre las eventuales advertencias y ataques que pueden afectar el sistema informático, donde partiendo del estudio se tendrán que diseñar una política de seguridad la cual otorgara distintas responsabilidades y pautas la cual se deberían seguir con el fin de escudarse de las distintas amenazas o ataques y así lograr desestimar los daños si se llegan a producir.

Es esta la razón que se debe definir hacia una dirección de prevención de un "archivo asequible que precisa las ordenes a disponerlas en materia de seguridad" (Villalón).[3]

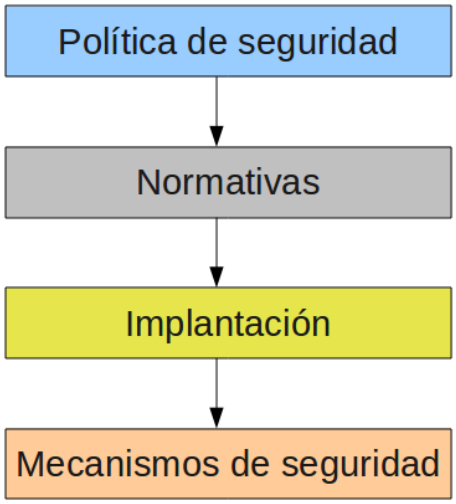

Ilustración 3

Fuente: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=4

[3] Villalon Huerta Antonio, 2007. Disponible en http://www.shutdown.es/seguridad.pdf

Las articulaciones de la protección están divididas en tres clases:

Advertencia:

Pueden ser todas aquellas acciones encaminadas a evitar cambios en relación a la habilidad de confianza.

Un ejemplo: es el uso de un cifrado conocido que ocasiona que un salteador a pesar de detener el ataque, no pueda entender la indagación en medio de una organización.

localización:

Permiten detectar las alteraciones, violaciones o intentos que se producen, a la protección del sistema.

Un ejemplo: Es el mecanismo Tripwire que es deteriorado para la seguridad en los archivos.

Restauración:

Son las acciones aplicadas cuando se ha detectado una vulneración a la protección del sistema con el fin de rescatar su funcionamiento normal.

Un ejemplo: el empleo de los plagios en la invulnerabilidad.

Los mecanismos en la separación, en función de cómo se fraccionan la intención, son divididos en los siguientes grupos: separación física, temporal, lógica, criptográfica y fragmentación.

- Dispositivo de protección en las conexiones.

En cuanto a la seguridad en la comunicación (integra y privada) se usan seguros tipo SSH o Kerberos, los cuales se encargan de cifrar el tráfico por la red.

Gracias a las Políticas de seguridad que se otorga a la información en nuestros sistema[4], se convierte en una forma eficaz de protección, logrando una estructura organizada que protege la información en nuestro sistema, precisando así una defensa conveniente.

[4] http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-segurida{d-informatica?start=4

La protección de datos en una organización es la garantía que pueden ofrecerle a sus usuarios, con esto se logra la continuidad de los distintos negocios que se tengan, mitigando este peligro se logra maximizar el retorno de inversiones y la creación de oportunidades de negocio.

La firmeza de la indagación se alcanza implementándolo a una agrupación apropiada de observación, incorporando direcciones, cursos, técnicas, disposición estructuras y competencias de software y hardware. Estos procesos requieren ser constituidos, implementados, observados, revisados, donde sean necesarios, para proteger que se ejecute su intención específica de asegurar el intercambio de la entidad. Esta responsabilidad debe realizarse en grupo con otras series de trámites de beneficio.

2.1.2 ¿DEBE SER NECESARIO LA SEGURIDAD DE LOS DATOS?

Si, ya que los datos que están guardados, alojados, en nuestros equipos, servidores, normalmente son información privada y muchas veces estos datos son usados para cometer cibercrimen, así como la información que una empresa puede tener en su sistema, como sus clientes, gustos, pedidos, alguien ajeno le gustaría obtener esta información con el fin de poder montar competencia en el ámbito de los negocios, con estos actos de cibercrimen lo que se logra fuera de causar los daños al extraer la información es la de perjudicar el buen manejo que pueda tener la estructura informática montada.

Los orígenes esenciales que llevan a esta problemática es la ineficacia de la protección que se está presentando en la parte de las empresas y agrupaciones en todo el mundo, y que no coexiste aprendizaje alternado con la planificación de un modelo de protección eficaz que asegure la demanda tecnológica de las vigentes advertencias combinadas.

En efecto, se considera delito el invadir un sistema de seguridad, reforma de las cifras o información almacenada, modificar las advertencias que puedan ser susceptibles de alguna estructura sea informática o no, las cuales pueden representar un deterioro o una problemática a futuro de gran dimensión.

Por racionalidad, la indagación, como los sistemas informáticos deben estar asegurados a cualquier ofensiva externa o interna que procure despojar, manejar o perjudicar los datos. Teniendo en cuanta lo estudiado, verificamos que no se puede asegurar que su protección sea adecuada, diga quien lo diga. Por seguridad es necesario implementar estrategias preventivas a cada una de sus actividades.

Cuantiosos métodos de asesorías no han sido planteados debidamente para ser fiables, generando que la protección que se logre por medio de los modos técnicos sea restringida y obliga a comprometerse a permanecer en una conducta apropiada.

El reconocer la observación como método de instrucción en conjunto con la colaboración de los empleados lograría una planificación y reflexión las cuales ayudarían a lograr una meta más clara con el fin de llegar a la inmunidad total.

Partiendo estos conceptos mencionados podemos plantearnos **cuáles son los riesgos y amenazas más frecuentes en el desarrollo del software seguro y como pueden evitarse**.

Lo primordial es realizar al inicio la implementación de la autenticidad en el manejo, con esto logramos saber y registraremos cuál es la información que se debe proteger, de qué forma podemos preservar, aclarándolas estarían seguros de los sujetos con los cuales se interactúa y de esta forma podríamos reducirlas llegando a una amenaza aceptable. De igual forma es muy necesario referir los distintos modelos de los periodos de desarrollo del software y almacenarlos en una base de con el fin de prevenir ataques futuros a otras aplicaciones.

La seguridad en el Software debe estar implícita desde el mismo diseño del software, ya que sería un error dejar la seguridad para etapas posteriores al desarrollo de software.

Para la seguridad se recomienda iniciar desde los requerimientos, los cuales no pueden ser sencillos, así como el hardware y software que se implementaran para los registros, como lo son los firewalls y antivirus, estos controles deberían dirigirse en orientación a la seguridad de la información crítica almacenada y así mismo para toda aplicación que se desarrolle se debe tener en cuenta la perspectiva y forma de pensar del posible agresor.

2.1.4 AMENAZAS AL SOFTWARE SEGURO

El software está sujeto a 2 categorías consideradas generalmente como ataques las cuales son:

Mientras su progreso: Alguna persona con conocimientos del sistema podría sabotear el programa durante su etapa de desarrollo.

Durante la operación. Un Usuario ajeno al sistema podría intentar sabotear el sistema durante su uso.

Software en la red: El software en la red siempre va a estar expuesto hacia la utilización de las distintas fragilidades, que se pueden derivar o clasificar de las siguientes formas:

- La complejidad del software o cambios posteriores que incluya el modelo de procesamiento

- Requisitos incorrectos por parte del desarrollador en donde se incluyen las relacionadas con la capacidad necesaria para el correcto funcionamiento, las salidas o periféricos de salida.

- Incompatibilidad en el planteamiento o condición de la apariencia del software con más aplicaciones visibles.

Se debe estimar los problemas que en primer lugar representan un riesgo al desarrollo del Software, así se determinan cuáles son los prioritarios y de esta manera se pueda llegar a una categoría, la cual nos va a permitir fijar con claridad y brindar soluciones y así identificar dónde se debe invertir mayor esfuerzo para corregir o mitigar el riesgo asociado.

2.1.4.1 COMO PREVENIR ESTAS AMENAZAS

La OCDE4 fomento en 1992 unas de Direcciones para la protección de los datos informativos, para impulsar el empleo y mejora en la sociedad creando una confianza, no solo en la mejora de estructuras y servicio de transmisiones, por medio de la aceptación de “nuevas estructuras de aceptación y comportamiento en el uso de la interconexión de esos sistemas”.

Los órdenes presentes son: razonamiento, compromiso, contestación Apropiada, moral, pluralismo, valoración de la amenaza, planteamiento y ejecución de la protección, diligencia de la protección, apreciación.

Con la transformación de los datos de la información y la manera de realizar intercambio, la comunicación se ha transformado eficazmente importante para los individuos y básicamente para el ordenamiento. “Los procedimientos, distribución y función de la comunicación, deben ser confiables e indudable, ya que proporciona que los individuos sean más subordinados.”

La finalidad que se busca es que las protecciones aplicadas a los datos sean para resguardar la privacidad, plenitud y recursos de los datos y de los bienes que la contienen o procesan. De tal forma, las estructuras e individuos se pueden proteger de:

- Propagación ilegal de datos que lamenten la seguridad y discreción, de apariencia casual o a favor, sin aprobación.

- Reformar sin previa autorización de manera casual en la cual se evidencie sin la debida a probación del poseedor.

- Desaparición de datos fundamentales sin probabilidad de rescatarla

- No poseer la probabilidad de los datos en el momento que se requiera. La indagación debe ser dirigida y custodiada apropiadamente de los peligros que confronte. El dato importante se puede tener en algunas estructuras: física, custodiada electrónicamente, transferirse en formas de masivas o alguna manera que se pueda trasladar, anunciar por métodos televisivos.

2.2. MARCO TEÓRICO

Almacenamiento documental. Se debe tener presente que el objetivo general de los medios de almacenamiento documental va desde la conservación, preservación, seguridad y consulta ágil y eficaz de los escritos primordiales, inclusive la reducción de la capacidad física o electrónica sin daño de los respectivos datos.

Referente al empleo del trámite en papeleo, ya que se ha manifestado un resistente contendiente a la microfilmación, esto es el almacenamiento magnético-óptico y la digitalización documental, que en la medida en que bajen sus costos y se estandaricen los productos, probablemente en un período de tiempo indefinible, asumirá el control de estos procesos empresariales.

Si bien es cierto que el uso de los actúales medios electrónicos de almacenamiento ofrecen probabilidad en la conservación de procesos de variada calidad, también cabe la responsabilidad el peligro que lleva con sus respectivos documentos por la rapidez de lograr este servicio, actualmente sin permiso se podrían cometer alguna confusión al analizar la respectiva información de un registro suspicaz según la manera que pueda ser almacenada en cualquier medio electrónico u óptico-magnético, introducir su estructura, su estilo o valide la información.

En la empresa, el Comité de archivo, el archivista y los auxiliares responsables, deben garantizar la implementación del proceso de almacenamiento documental, así se logrará una rentabilidad útil en la conservación de la demanda, en todo caso, segmentar la aplicación de los fundamentos archivísticos garantizará la protección del patrimonio documental.

Concepto de almacenamiento documental. El almacenamiento documental lo podemos identificar como la implementación de una serie de procedimientos técnicos y lógicos que garanticen la protección, preservación y conservación de la información empresarial, soportados en medios técnicos universalmente aceptados, entre los cuales podemos citar los siguientes: archivos físicos organizados, micro-filmación, memorias USB, CD, DVD, discos duros y, más recientemente, en "La nube" almacenamiento virtual[5].

Medios de almacenamiento documental. Las técnicas de almacenamiento documental son variadas y las alternativas aumentan en la medida que avanzan los desarrollos tecnológicos. En la actualidad se cuenta con sistemas de almacenamiento documental completamente tecnificados e integrados, como es el caso de los computadores integrados en la red por medio de bases de datos y la virtualidad, que permiten minimizar, a cuestión de segundos, la duración de ingreso a la documentación que requiere. Sin embargo, es importante resaltar que se siguen utilizando medios que son irremplazables como los archivos físicos (papel) y la microfilmación.

A continuación, realizamos una breve descripción de los medios de almacenamiento más usuales, así:

Archivo físico documental. El archivo en medio de almacenamiento físico, fue el primero que se utilizó y se sigue utilizando en la actualidad, bajo una serie de parámetros técnicos y organizacionales, teniendo como soporte medios lógicos como apoyarse en la información y documentos en la consulta sistematizados, enmarcados en la función SENO, es decir[6]:

S = Seguridad.
E = Estética.
N = Normatividad.
O = Operatividad.

Microfilmación. La microfilmación es un medio de almacenamiento documental en películas fotográficas, que utiliza diversos grados para la reducción de imágenes, por lo que requiere aparatos ópticos para su ejecución y observación. En otras palabras, los microfilms son imágenes reducidas mediante sales de plata de 16, 35, 70, y 105 mm de ancho, adoptando la presentación final mediante micro formas, las cuales dependen de las características y uso que se quiera dar a la información, siendo las más comunes: el rollo, el cartucho, los casetes y las micro fichas[7].

---

[5] Ibíd. ISO 27001 p. 64.

[6] Ibíd. ISO 27001 p. 65.

[7] GÓMEZ CARDONA, William Darío. Prácticas empresariales. Ecoe ediciones. Primera Edición. Bogotá, D.C. Colombia. 2012. p. 65.

En la actualidad esta tecnología está completamente desarrollada y complementada por sistemas de digitalización de imágenes soportados en grandes bases de datos para agilizar la consulta y la exactitud de la información.

Manual para la administración de archivos[8]:

Objetivo: Por la importancia que tiene como memoria empresarial, toda empresa o institución sin importar el tamaño o su carácter público o privado, debe disponer de una herramienta que le permita adquirir y mantener la capacidad de organizar administrativa y técnicamente una dependencia para la administración de documentos de todo tipo, aplicando principios claros de selección, conservación y descarte documental, de acuerdo con las políticas internas, los documentos propios de cada empresa y la legislación que regula este proceso.

2.3. MARCO CONCEPTUAL

2.3.1 LA SEGURIDAD INFORMÁTICA

Todas las estructuras informáticas deben dedicarse al desarrollo de la seguridad en y durante el intercambio de información, en el cual se dispone una comunicación continua, segura y con posibles periodos de inseguridad, con esto logramos establecer una utilidad en donde poseer datos es obtener el dominio de la información.

El análisis es imprescindible para avalar la prolongación operaria de la estructura, un eficaz equipo gremial la cual su garantía tiene una importancia para sí misma que deba corresponder individuos que precisan la información. El sistema debería proteger la privacidad y seguridad de su respectiva información para que sean solo accesibles a individuos autorizados para preservar la información, que no permita los ingresos que no estén autorizados, la seguridad informática no puede ser algo opcional, si su seguridad no es la adecuada esta puede tener graves consecuencias en varios entornos, tanto laborales como representativos;

- La responsabilidad cívica o representante.
- Ética
- Aceptable
- La acreditación en cuanto a la seguridad.
- Daño a bienes.
- Documentación e información que no se puedan recuperar
- Datos privados expuestos
- Pérdidas en explotación.

[8] GÓMEZ CARDONA, William Darío. Prácticas empresariales. Ecoe ediciones. Primera Edición. Bogotá, D.C. Colombia. 2012. p. 53.

Los riesgos, se deben intervenir de una manera preventiva, con el fin de proteger la privacidad, en la planeación o pensamientos relacionados con la seguridad se debe considerar lo siguiente:

Determinar los permisos de los usuarios por un nivel de confianza, al conceder esto se logra asegurar cada modelo o fase con el fin de garantizar un desarrollo seguro.

Si las competencias previas no son valoradas adecuadamente al producir y establecer un procedimiento de protección único, será un desarrollo en vano, ya que no se llevará un ciclo, proceso o escalamiento de la seguridad expresada.

2.3.2 ADVERTENCIAS DE LA SEGURIDAD EN LA INFORMÁTICA

- El beneficiario que consecuente o instintivamente origina una incógnita de protección informática.
- Programaciones malignas como: virus, troyanos, programas espía, botnets, etc.
- Un extraño que logra entrar al sistema o programación en el cual no se le permite la entrada.
- Un acontecimiento de carácter tipo desastre natural o manipulado por la mano del hombre la cual ocasiona la desaparición de los respectivos datos.

2.3.3 MODELO DE AMENAZA

ADVERTENCIAS METODOLOGICAS:

Premeditados por virus, malware, el desgaste del mecanismo al ingresar sin aprobación del software inadecuado lo cual pueden proceder confusiones de maneras instintivas por programación.

ADVERTENCIAS TANGIBLES:

Error en el mecanismo de desastres tipo sismo.

EN QUE MANERA SE PUEDE ADAPTAR LA INMUNIDAD EN LA INFORMATICA.

Usualmente en la protección se ha especificado respaldar la entrada de documentos y medios de la estructura, conformando las herramientas originales que garantizan a los beneficiarios de estos medios que son los únicos en gozar este derecho que fue entregado.

LA PROTECCION DE LA INFORMATICA SE PUEDE RESPALDAR.

- Las reservas de los datos en la información.
- La recuperación eficaz y completa de las estructuras de los respectivos datos.
- La plenitud de los datos.
- La privacidad de los datos.

NUESTRA PROPOSICION

- Contemplar la legalidad de la protección en la Informática.
- Reconocer la dificultad.
- Mejora en el programa de protección en la informática.
- Observación de la protección de conjuntos en la computación.
- Inicios en la protección en la Informática.

SINGULARIDADES:

En la informática la protección es apoyarse en la manifestación de la estructura de los respectivos datos en cuanto elemento informático o en esquema ante un posible ataque, al formar y emplear de manera adecuada la entrada a la información contenida, siendo de forma admisible por medio de individuos a los cuales se les autoricen sus límites de su licencia o privilegios para que así la estructura corresponda a ejecutar posteriormente las posibles soluciones.

Generalidad: Característica obtenida la cual no permite que sea cambiada por aquellos individuos que no se les permita su acceso.

Privacidad: es la generalidad, atributo para aquellos que poseen el permiso, que solo ellos podrán ver, acceder a esa información.

UTILIDADES

- La protección informática confía en la seguridad, la plenitud y confidencialidad de la información de una estructura.

- Diseñar oportunas normas de protección que previene destrucción y preocupaciones que alcanzar algún extraño.

- Diseñar escudos de protección que pueden ser de tecnologías aplicativos y mecanismos de confianza y solidez modelos como: Corta fuegos, Antivirus, Anti espías encriptaciones y uso de contraseña que son las que favorecen la información y los conjuntos de los beneficiarios.

PERJUICIOS:

Una protección completa no puede ser posible, los antivirus cada vez tienen problemas para la detección de software maligno, los requerimientos para la producción de contraseñas deben ser más difíciles.

LOS DESAFIOS QUE INDISPONEN LA DEFENSA DE LA INFORMÁTICA

Inspeccionar la navegación de los beneficiarios, disponer reglas que usualmente empleen en el servicio de entrada a estas Redes Sociales, Facebook, Twitter, Visualización de videos y TV, YouTube, Escuchas de audio, Spotify, radios online, Juegos Online, Farm Ville. Mensajería instantánea: Skype, Messenger.

Descargas P2P, Emule, Torrent, Megaupload manipular el escape de los datos Correos privados, Gmail, Hotmail, uso de dispositivos de almacenamiento externos como Pen Drives USB, no tener la información encriptada.

Alertas ofensivas de hackers, virus, etc., moderar el montaje de un **firewall UTM** que integran algunas funciones en un único sistema, Concientizar a los beneficiarios de los inconvenientes asociados con la protección informática.

2.4. ANTECEDENTES

Título: “CREACION DE UNA ESTRUCTURA ADMINISTRATIVA DE PROTECCION DE LA INFORMACIÓN PARA ASISTENCIA DE CORRESPONDENCIA DEL PERÚ S.A.”

Autores: David Arturo Aguirre Mollehuanca
Recopilación

La reclamación de herramientas para las reglas practicas peruana NTP-ISO/IEC 27001:2008 en los entes territoriales del estado se forma de acuerdo a la obligación de administrar apropiadamente con firmeza de lo ilustrativo en los distintos negocios. Sin bloqueo a lo alterado en materia, sin lugar a duda la admisión, ha considerado que no se tenga en cuenta ciertas disipaciones para garantizar la culminación del proyecto en espacio acordado por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) ente encargado de asistir empresas publicas mientras el procedimiento de implementar reglas. Oportunamente para ello se ejecuta este proyecto con el fin tipo carrera para resolver, obrar con un ente público a manera de tema y análisis a fin de crear una estructura administrativa en protección, empalmando a las reglas donde así ajustar la disposición proyectando, en un porvenir, valer como advertencia en la promulgación del mismo. En efecto, se llevaron algunas sesiones con la admisión directrices que permitan fijar el alcance y las políticas del SGSI en la estructura encaminar en cursos institucionales apreciación en auge de identidad, luego una sucesión de encuentros que accediera identificar y valorar los activos críticos de la organización, así como identificar y evaluar los riesgos a los cuales estos estaban sometidos. Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles de la NTP ISO/IEC 17799:2007 se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la estructura.

NOTA

Es justo anunciar las normas de seguridad existentes y constituir diálogos de capacitación y concientización en toda la empresa, es preciso a la ausencia de culturización en protección que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.

Título: “ESTRUCTURA DE INTERCEPTACIÓN Y OBSERVACION DE COMUNICACIONES”

Autores: Carlos Gacimartín García

Resumen

Se pretende diseñar una solución hardware y software para facilitar el análisis de tráfico de una conexión a Internet por las fuerzas de seguridad sin intervención ni conocimiento necesario del ISP. El tráfico generado por un usuario en Internet se intervendrá y analizará, y según unos baremos se ponderará para crear alarmas que indiquen una actividad sospechosa, de cara a requerir mayor atención por parte de las autoridades. Para ello se planteará el hardware y software necesarios, desarrollándose además el núcleo o core del software con facilidades para que pueda mantenerse y ampliarse. Mediante la captura de todo el tráfico de red de un individuo, se realizarán en tiempo real y solapándose las siguientes tareas: 1.- Realizar un primer análisis de la información generando alertas ante determinados contenidos detectados. (nivel INDECT WP3) 2.- Almacenar todo el tráfico de red capturado y reenviarlo a un servidor propio. 3.- Realizar un análisis más detallado mediante la decodificación completa de los protocolos deseados (nivel INDECT WP4) utilizando para facilitar su estudio por un operador

NOTA:

Funcionamiento en tiempo real: dada la naturaleza de la actividad, la obtención de información sobre amenazas es vital, y se ha de conseguir en el mínimo tiempo posible para poder reaccionar a tiempo. Para ello se han utilizado las tecnologías más avanzadas y se han realizado pruebas de laboratorio, a expensas de las pruebas reales, obteniéndose alarmas en tiempo real.

A su vez diseñar el sistema de modo que no se pueda dar cuenta el espiado: por lo que se ha optado por la arquitectura en modo sniffer frente a bridge, y tecnologías que en ningún modo puedan alterar el funcionamiento de terceros. Así mismo se ha optado por blindar el prototipo de modo que sea prácticamente invulnerable, con los medios actuales, a su disección

Título: “PROGRAMA DE CONCIENTIZACIÓN EN SEGURIDAD DE INFORMACIÓN EMPRESARIAL”

Autores: Ing. Luis Lunar

Resumen

La concientización en el área de seguridad de la información es un proceso de enseñanza-aprendizaje para cambiar la conducta o manera de actuar de las personas mediante el entrenamiento y la educación, a los fines de minimizar sus vulnerabilidades, y proteger a la organización contra las amenazas que pueden aprovechar esas vulnerabilidades. Este proceso de aprendizaje tiene gran importancia en las empresas, debido a que las personas, como entes que crean, administran e interactúan con los sistemas de información empresarial, son potencialmente vulnerables a las amenazas en contra de la seguridad de la información, en virtud de que durante el desarrollo de sus actividades diarias están expuestas a errores, omisiones, fraude, abuso y acciones destructivas, originados dentro y fuera de la organización. Esta situación fue la que motivó la presente investigación cuyo objetivo general es diseñar un programa de concientización en seguridad de información empresarial. Para tal fin se aplicó una metodología de tipo documental que presenta un enfoque cualitativo de diseño no experimental de una investigación-acción. La investigación utilizó como principal soporte teórico la Guía del usuario: elaborar programas de sensibilización sobre la seguridad de la información de Charles Cresson Wood (2006). Finalmente, como conclusión principal se obtuvo la siguiente: las bases de un programa de concientización, sensibilización y educación en seguridad informática empresarial, están constituidas por el enfoque de gestión de cambio, la responsabilidad compartida del personal, la situación antes de la aplicación, el costo, el apoyo de la alta gerencia, y, por último, la gestión del programa mediante los procesos de planificación y valoración, ejecución y gestión, y evaluación y modificación.

NOTA:

La concientización en seguridad de información empresarial es un programa que tiene como objeto el resguardo contra amenazas y vulnerabilidades tecnológicas, mediante un enfoque de entrenamiento y educación apropiada que conduzca al desarrollo de una cultura de seguridad de la información; donde el personal adopte la política de seguridad de la organización, la respalde durante la ejecución de sus tareas normales, y tenga la sensibilización para responder segura e intuitivamente a la acción de agentes que pongan en riesgo la seguridad de la información, en cualquiera de sus dimensiones: confidencialidad, disponibilidad e integridad.

Las personas, como entes que crean, administran e interactúan con los sistemas de información empresarial, son potencialmente vulnerables a las amenazas en contra de la seguridad de la información, en virtud de los errores, omisiones, fraude, abuso

y acciones destructivas, originados dentro y fuera de la organización. La vulnerabilidad de las personas está en función de su capacidad de aplicación preventiva y correctiva de medidas de seguridad y de responder apropiadamente en caso de un una potencial amenaza o vulnerabilidad.

Mediante la concientización se cambia la conducta o manera de actuar de las personas en el ámbito de seguridad de la información para lograr minimizar sus vulnerabilidades, protegiéndolas contra las amenazas que pueden tomar ventaja de ellas, y llevándolas al nivel más eficaz en la defensa de la información de la organización. La sensibilización es el grado de respuesta apropiadamente para aplicar medidas de seguridad preventivas y correctivas y en caso de un una potencial amenaza o vulnerabilidad, se logra mediante programas con enfoque de gestión de cambio. Los planes de entrenamiento y educación deben tener como meta el desarrollo de una cultura de seguridad de la información.

Las bases de un programa de concientización, sensibilización y educación en seguridad informática empresarial, están constituidas por: la adopción de un enfoque de gestión de cambio; inclusión de todo el personal, la seguridad como responsabilidad de todos; el establecimiento de un punto de partida teniendo en cuenta la situación actual antes de su aplicación; la gestión de los procesos de planificación y valoración, ejecución y gestión, y evaluación y modificación; el costo del programa; y finalmente, lograr el apoyo constante de la alta gerencia como factor de éxito. El soporte de la alta gerencia al programa es de vital importancia a los fines de: permitir la definición y servir de ejemplo para la divulgación de las políticas corporativas, proveer recursos, agilizar los procesos, aplicar todas las normas establecidas, y facilitar el seguimiento de la gestión.

Título: “SISTEMA DE INFORMACIÓN ADMINISTRATIVA”

Autores: Natalia Rodríguez

Resumen

La manera en que manejamos la seguridad de la información ha evolucionado con el tiempo, este desarrollo ha sido gracias a la constante globalización, la constante investigación y desarrollo de nuevas y mejores tecnologías que hacen que las empresas y las personas se vean favorecidas, algo muy importante hoy en día es la recopilación, análisis, y tratamiento de la información, esta debe ser constantemente revalidada y protegida de la mejor manera. , a medida que nuestra sociedad y tecnología evolucionan, por ello es importante comprender esta evolución para entender como necesitamos enfocar la seguridad informática en la actualidad, ya que lo que en algún momento es seguro con el paso del tiempo ya no lo es.

En el presente informe se dará a conocer que es la seguridad informática, las posibles amenazas que se están expuestos y por lo tanto se debe usar la seguridad informática, estándares de seguridad informática, certificaciones en ISACA, diferencias entre seguridad informática y seguridad de la información

NOTA

Una vez realizado este trabajo investigativo puedo decir que la seguridad informática juega un rol importante para el resguardo de toda la información que se recopilan en las empresas y también las personas normales, el mal uso de esta puede generar graves daños y problemas, es por eso que se debe estar constantemente asegurando toda la información que tienen las personas y empresas.

La seguridad informática es muy importante para las organizaciones porque se preocupa de proteger toda la información que se maneja por lo tanto es de vital importancia estar preocupado de que este seguro.

Teniendo en cuenta la relación de todos los autores anteriores, se puede establecer que las mejores prácticas recomendadas para el desarrollo y ejecución del programa de concientización, sensibilización y educación en seguridad de la información empresarial son: norma ISO/IEC 17799 que establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión; ISO/IEC 27001 especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información; los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT) que establecen un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos; la Guía del usuario: elaborar

programas de sensibilización sobre la seguridad de la información de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) que ilustra los principales procesos para planificar, organizar y poner en práctica iniciativas de sensibilización; Políticas de Seguridad Informática. Mejores Prácticas Internacionales de Charles Cresson Wood es un conjunto completo de políticas de seguridad informática.

Muchos de los planteamientos y problemas en seguridad informática se encaminan a protegerse contra accesos no autorizados, pero este es un problema sencillo de resolver, ya que durante años se han desarrollado y perfeccionado algoritmos matemáticos para el cifrado de datos, para el intercambio seguro de información, para garantizar el correcto funcionamiento del software, que se ha [9]traducido en herramientas capaces de proporcionar soluciones rápidas y sencillas a problemas técnicos de seguridad. Desafortunadamente, no es suficiente simplemente arreglar los errores o eliminar las fallas técnicas de seguridad.

El problema va mucho más allá. La Seguridad Informática es un problema cultural, en el que el usuario juega un rol protagónico. La metodología para el aseguramiento de entornos informatizados - MAEI2, resalta la importancia de tener una metodología clara para realizar un análisis de riesgos e identificar claramente vulnerabilidades, riesgos y amenazas presentes en los activos de información, ser gestionados y que permita optimizar los procesos organizacionales. De igual forma también la existen lineamientos establecidos en la norma internacional UNE/ISO 27001, que establece las especificaciones para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). Esta norma establece un enfoque por procesos basado en el ciclo Deming, que plantea la gestión de la seguridad como un proceso de mejora continua, a partir de la repetición cíclica de cuatro fases como lo son planificar, hacer, verificar y actuar. Dentro de las especificaciones de la norma se establece un esquema documental del SGSI, que debe mantenerse actualizado, disponible y enmarcado en un índice, especialmente si la empresa desea superar un proceso de certificación, tal como lo describe un proceso de implantación de un SGSI3 , el cual expone claramente los lineamientos que deben seguirse para implantar un Sistema de Gestión de Seguridad de la Información en un entorno real, describiendo el proceso para realizar el análisis de riesgo y sus fases futuras.

[9] 1 PALLAS MEGA, Gustavo. Metodología de implantación de un SGSI en un grupo empresarial jerárquico. Universidad república de Montevideo (Uruguay), 2009.

2.5. MARCO LEGAL

2.5.1. Constitución Política Artículo 15. Reconoce como Derecho Fundamental el Habeas Data **Artículo 20.**Libertad de Información
2.5.2. Ley 527 de 1999. "Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
2.5.3. Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países
2.5.4. Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"
2.5.5. Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la Protección de Datos Personales"
2.5.6. Ley 1621 de 2013 "Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones"
2.5.7. Ley 1712 de 2014"Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones
2.5.8. Decreto 1727 de 2009 "Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información"
2.5.9. Decreto 2952 de 2010 "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"
2.5.10. Decreto 1377 de 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"
2.5.11. Decreto 886 de 2014 "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
2.5.12. Código Penal Art. 199. Espionaje Art. 258. Utilización indebida de información

Art. 418. Revelación de Secreto
Art. 419. Utilización de asunto sometido a secreto o reserva
Art. 420. Utilización indebida de información oficial
Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública
Artículo 463. Espionaje

2.5.13. Política Pública
2.5.14. Documento Conpes 3701
2.5.15. Lineamientos de Política para Ciberseguridad y Ciberdefensa
2.5.16. [10]Entidades Responsables:

Ministerio de Interior y de Justicia
Ministerio TIC
Ministerio de Defensa Nacional
Departamento Administrativo de Seguridad
Fiscalía General de la Nación
Juzgados Penales

[10] 29 feb. 2016 - II. Marco legal. Seguridad de la información y medidas de seguridad.

3. DESARROLLO DEL PROYECTO

CAPITULO I. **Riesgos y amenazas en el desarrollo del Software Seguro**

Lo primordial en la creación de software seguro es saber cuál es la estructura que se va a llevar para la seguridad, la forma en que se deben proteger los datos, con esto se podría llegar a mitigar amenazas hasta el punto de llegar a disminuirlas, con esto se lograría un periodo vital en el desarrollo de software.

Durante el desarrollo de software podemos encontrar factores tecnológicos y humanos los cuales conllevarían amenazas que pueden generar perdida y uso indebido de la información extraída.

Factores Tecnológicos

En los factores tecnológicos, encontramos los comunes como las fallas de hardware o software, falla en el suministro eléctrico y ataque por parte del malware.

Ataques tipo Malware: Este tipo de ataques tienen como objetivo el perjudicar el manejo del computador, sin su autorización o la instrucción del beneficiario. Este tipo de ataques habitualmente, cambian los archivos ejecutables por otros que se encuentran infectados. De igual forma pueden destruir, de forma intencionada la información almacenada en el computador, así mismo existen otros tipos de malware que son inofensivos, en donde lo único que quieren es molestar al usuario.

Deficiencias tangibles e intangibles: Las principales deficiencias del hardware que podemos encontrar son las que tienen que ver con: fallas de memoria RAM, calentamiento del procesador por falta de ventilación o falla de algún componente del equipo, y como las principales fallas de software podemos encontrar: fallas del Sistema Operativo, presencia de virus, conflicto que tienen que versión con la arquitectura del programa, estas fallas que encontramos nos pueden retrasar en la entrega, producción, verificación y solución a los errores durante la creación del software.

Falla en el servicio eléctrico: Estas fallas a pesar que no son de responsabilidad humana, si tiene que ver con el desarrollo de software, ya que se puede presentar una sobrecarga en el sistema eléctrico el cual podría afectar los equipos en donde se está desarrollando el software debido a que perjudica esencialmente el hardware, que mencionamos con anterioridad.

Factores Humanos

Acá podemos mencionar los factores más destacados hechas por la mano del hombre; como lo son los crackers y hackers, los cuales están más relacionados con la Seguridad que tengamos en la red donde se esté desarrollando el software, pero no son solo estos los que puedan ocasionar daños o interferir en el desarrollo del software seguro, ya que la misma competencia podría invitar a alguno de los desarrolladores a su empresa, ofrecerle dadivas con el fin de hacerse con el software que se esté desarrollando y logrando esto podría sacarlo más rápido al mercado, hacer mejoras que él tenga en mente o en su defecto podría pedir solo que se infecte el sistema y tener una pérdida del sistema.

CAPITULO II. **Periodo vital de un software y su uso en su progreso de un programa de software.**

Los ciclos vitales de software son conjuntos usados y empleados en la sociedad durante el progreso del software, con el fin de diseñar servicios en cualquier plataforma y de cualquier índole, logrando así que sean convincentes y aceptables en el momento de emprender el desarrollo de software.

Existen diversos modelos que nos llevan al establecimiento de un proceso con el fin de llegar al desarrollo de software, cada modelo nos describe un enfoque distinto para las diferentes actividades que se tienen durante el desarrollo del software.

Es muy importante la incorporación de estas técnicas de desarrollo las cuales deben ejecutar privacidad, plenitud y reserva teniendo en cuenta que sean fiables son.

El relacionarse por un periodo lleva a realizar repetidamente el mismo proceso para efectuar mientras el ciclo vital de su servicio.

El desarrollo intangible en cuestión de restablecimiento importante en la operación conveniente en su mayor parte necesita admisión en el manejo en su ejecución habitual.

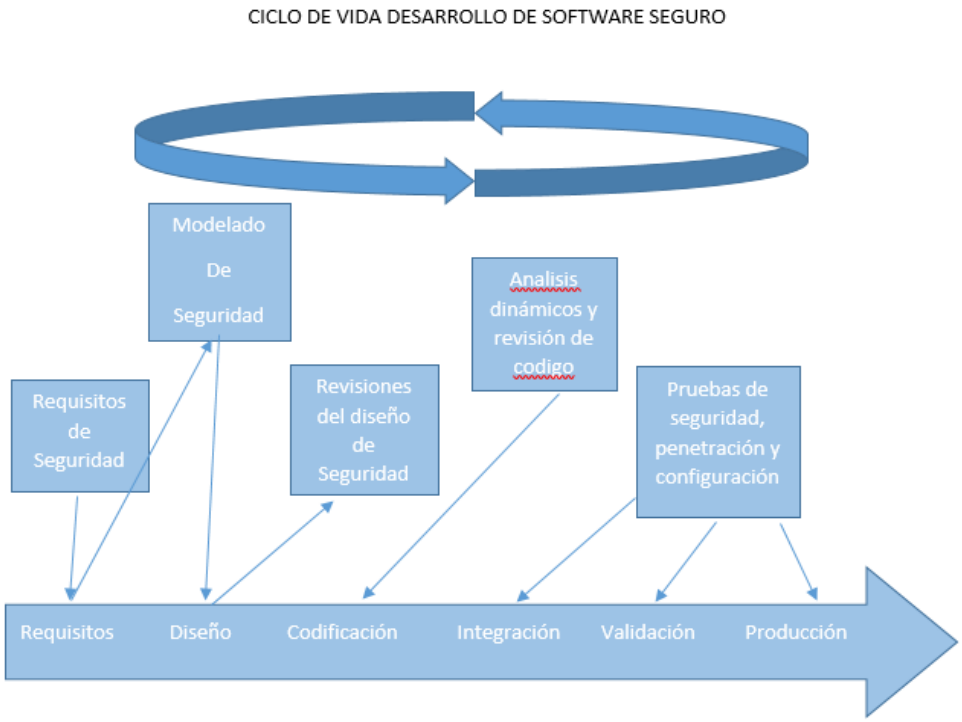

Ilustración 4

CAPITULO III. **La Metodología Security Requirements Engineering Process su funcionalidad y aplicabilidad para el desarrollo de software.**

La Metodología Security Requirements Engineering Process también conocida como SREP es un proceso el cual se basa en activos y dirigido para la creación de requerimientos de protección en el proceso de un Sistema de Información Seguro, esta metodología es la herramienta de Common Criteria "CC", el "CC" es un estándar internacional ISO/IEC 15408 el cual habla sobre seguridad informática en las distintas etapas del proceso de creación de software, donde su meta es determinar los requerimientos que sean necesario a los diseñadores del software determinar los rasgos de garantía y así mismo poder estimar sus resultados efectuar su objetivo.

SREP describe como integrar los periodos vitales de un Software Seguro en su etapa de progreso cerca con la utilización repositorios para la protección facilitando la reutilización de requisitos, activos o bienes, amenazas y soluciones a un error planteado.

Así misma está centrada en la construcción de conceptos que tienen que ver con la protección en primera clase de su crecimiento logrando así de esta forma, el modelo elegido sea repetitivo y ampliado, logrando así que dichos requerimientos de

protección y los fundamentos relacionados evolucionen a través del periodo de vital desarrollo, brindando soluciones que a su vez que se tratan distintas obligaciones eficaces y no eficaces del Software.

Esta metodología de manera genérica puede ser descrita como un complemento de actividades, el cual se podría integrar sobre un modelo de cualquier organización logrando así un enfoque hacia los requisitos de seguridad.

De esta manera, podemos decir que esta metodología es un proceso en espiral y los requisitos de seguridad y sus sistemas asociados se encuentran en constante evolución a lo largo del ciclo de vida del software, así mismo se van verificando otros requisitos funcionales y no funcionales.

Con todo lo que hemos hablado sobre la metodología SREP podemos determinar que la integración de la seguridad en las primeras fases del desarrollo de los Sistemas de Información es muy necesario si queremos construir sistemas de información seguros. Aun así, es fácil encontrar que esta seguridad se trabaja o trata cuando el sistema ya se encuentra diseñado y en funcionamiento al usuario final.

Es por esto que la Seguridad Informática es una disciplina que se encuentra en crecimiento como una importante rama de la Ingeniería del Software, debido a que estamos comprendiendo que la seguridad se debe abordar desde la fase de requisitos para el desarrollo y no como se mencionaba anteriormente cuando se encuentre en funcionamiento.

Esta metodología al ser un proceso en espiral podemos decir es la adecuada para el desarrollo de software seguro ya que describe el ciclo de vida de un software por medio de una espiral, la cual se repite hasta que se pueda entregar el producto final, logrando así que el producto se trabaje continuamente y las mejoras que se realicen a menudo tienen se realizan en pequeños pasos, una característica positiva de la metodología SREP y el uso del proceso en espiral es la minimización de los riesgos que se pueden encontrar durante el desarrollo de software, lo que podría generar un aumento de los costos, más esfuerzo y una puesta en funcionamiento retardada. Para minimizar estos riesgos se lanzan, prototipos, se realizan simulaciones, pruebas de referencia o entrevistas y/o encuestas con los usuarios que van a usar el sistema, en donde luego retornaran por las fases de desarrollo para corregir o mejorar las falencias encontradas.

Todos estos procedimientos son revisados y estructurados de manera diferente, ya que no todos los usuarios que realizan las pruebas van a encontrar las mismas falencias que el otro y al estar estructurados o revisados de manera diferente permite la corrección de varios problemas al tiempo y desde distintos puntos de vista.

CONCLUSIONES DE LA PROPUESTA

Después de realizar la investigación se busca dejar un documento donde se contextualice las amenazas más comunes usadas por el ciberdelincuente a las cuales están expuestos los usuarios y así mismo las formas, técnicas o métodos más comunes que se están usando para evitar o ya en caso extremo de corregir estas amenazas en el ciberespacio, todo esto con el fin de preservar la información que se almacena en el sistema, así mismo se deja expresado de cuál sería la mejor alternativa que nos ayudaría en el desarrollo y posterior entregar de un Software seguro, esta Metodología es la Security Requirements Engineering Process la cual es la más adecuada y recomendada, dado que esta se basa en la aplicación de la seguridad informática en las distintas etapas del proceso de creación de software, cumpliendo de mejor forma con las necesidades que se podrían presentar.

De igual forma se propone como refuerzo una charla en forma de capacitación por parte de los desarrolladores del sistema con los usuarios finales, con el fin de concientizar sobre los distintos peligros a los cuales están expuestos al manipular un equipo de cómputo con acceso a internet, sin clave de acceso, ya que no sirve que el Sistema que se cree tenga todas las medidas de seguridad si el usuario que lo manipula no tiene precauciones personales en lo que a seguridad informática se refiere.

Es fundamental que se continúe con el estudio de las tecnologías de la información, esto debido a las distintas soluciones informáticas que se van desarrollando diariamente y de igual manera se van desarrollando nuevas amenazas, generando así un cambio en las variables de riesgos de acuerdo al uso adecuado o inadecuado de la información, la información contenida en esta monografía será para contribuir a un soporte general de los distintos modelos que existen para la creación de software seguro, con esto se justifica la implementación de estrategias que abarquen las seguridad informática, teniendo en cuenta los distintos factores mencionados en la monografía.

Para tener en cuenta, durante el segundo trimestre (abril, mayo, junio) de 2018, los especialistas de Kaspersky Lab, empresa dedicada a la seguridad informática, detectaron 1.744.244 paquetes de instalación maliciosos, 421.666 más que en el trimestre anterior, con esta cifra podemos dejar claro lo antes mencionado, que las amenazas se desarrollan diariamente.

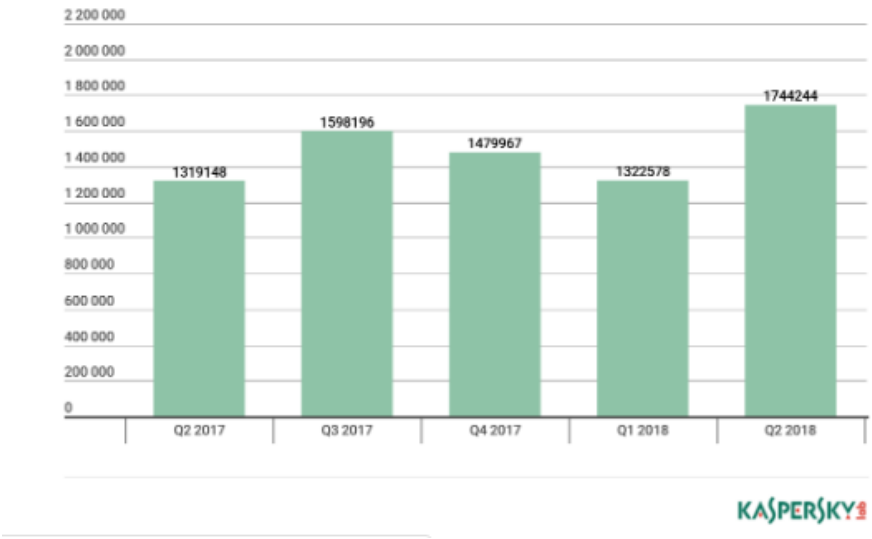

Ilustración 5

Número de paquetes de instalación de malware detectados, segundo trimestre de 2017 – segundo trimestre de 2018

Fuente: https://securelist.lat/it-threat-evolution-q2-2018-statistics/87391/

Con esta información podemos evidenciar que las amenazas informáticas están lejos de disminuir para todos los sectores informáticos, esto es entendible debido a que el proceso de globalización demanda el uso de la tecnología para cualquier transacción, en donde muchas veces no logramos prever los riesgos, debido a que estas amenazas evolucionan, se adaptan al actual mercado y a su próxima víctima.

Este tipo de resultados se evidencian porque las empresas no destinan una parte de sus recursos para le seguridad informática, estos recursos se emplean en la producción de activos y al hacer esto no se garantiza una protección adecuada de estos activos, muchos de los errores que se cometen en las empresas se debe a que subestiman el valor de los activos o información que poseen o sencillamente son ignorados.

CONCLUSIONES

En esta investigación monográfica se le dio luces a nuestra sociedad de cómo puede llevar a cabo la protección de sus datos, información importante, como también a conocer cada método existente, las amenazas a las cuales nos encontramos expuestos a diario cuando usamos las redes, así como también de que es lo que se debe proteger cada una de las personas para no ser perjudicados con su información y exponerse a que se haga un mal uso de las mismas.

Al dejar claro las etapas necesarias y la importancia que tiene el desarrollo de software teniendo en cuenta la metodología Security Requirements Engineering Process (SREP) la cual esta basada en activos y se orienta a los riesgos, lo cual permite establecer requisitos de seguridad mientras estamos desarrollando las aplicaciones, con este método se logra la implementación de un estándar de seguridad como lo es ISO/IEC 15408 durante las distintas fases del desarrollo del software, con estos se definen los requisitos de seguridad para los desarrolladores con el fin de especificar y evaluar que su desarrollo si cumplen con el cometido, debido a que esta metodología trata a cada fase del desarrollo como un mini proceso, en donde se aplican todas las actividades de la metodología las cuales nos permitirían identificar y mantener actualizados los distintos requisitos de seguridad por fase de desarrollo y al tener esto así se pueden mitigar los riesgos posteriores.

Se dejó claro sobre los distintos riesgos y las amenazas que existen para el software, los cuales van desde los desastres naturales, pasando por personal cercano al desarrollo el proyecto, los cuales pueden sustraer o sabotear información debido a algún mal entendido o por diferencias con el personal, así como personal que no tiene nada que ver con el desarrollo sino que pasan su vida haciendo daño de forma remota o con la creación de programas los cuales afectan o sustraen información precisa, dentro de estos programas dejamos en evidencia los más comunes en nuestro diario vivir, así como los nombres de las técnicas que los ciber delincuentes usan para implantar estos programas, las cuales van desde enviar un email el cual contiene una dirección la cual al abrir descargara el programa malicioso y se ejecutara sin que el usuario final tenga conocimiento de que es víctima de un ciberataque.

Afortunadamente para estas amenazas existen en el mercado software y hardware (Antivirus, Firewall, Antimalware, Antispyware), los cuales nos brindan soluciones completas, aunque muchas de las soluciones que nos brindan estos programas las podemos encontrar en nosotros mismo como primera barrera ante un ataque, dado que somos nosotros los que inconscientemente ejecutamos, abrimos o ingresamos a sitios de dudosa reputación, dejamos nuestros equipos sin clave para el ingreso al sistema en donde esta debe ser una de las primeras medidas para evitar que usuarios o personal ajeno al uso de nuestro equipo ingrese y pueda ejecutar ya sea inconscientemente o con uso de razón programas que causaran daños a nuestra información.

Se estableció de manera clara la terminología que es usada dentro de las estructuras de la información, como también en la protección informática, lo cual le permite a cualquier persona que sea (dumis, principiante o no), a conocer el nombre real de cada riesgo, la manera en que aplica el infractor informático los daños a nuestro sistema de información. Dando con esto que la sociedad sea más segura cada día, pueda usar aún más las redes, pueda proporcionar sus datos con confianza, y pueda llevar a cabo transacciones con información de interés.

Así mismo se establecieron las etapas o ciclos que se deben tener en cuenta al momento de la creación de un software seguro, donde se abarcan principios básicos como la privacidad de la información, esto con el fin de siempre de lograr la protección de la información en nuestros equipos; pero para la lograr la solución de estos se debe empezar con analizar los requisitos que se necesitan y el personal o equipo de trabajo que lo llevara a cabo con el fin de pasar a la infraestructura tecnológica necesaria para el desarrollo del software, ya con estas etapas se llega a la parte donde se habla de la metodología que más nos sirve y llegar hasta la implementación en donde se le retroalimenta al personal de desarrollo las fallas evidenciadas y las mejoras que se podrían implementar.

La metodología Security Requirements Engineering Process (SREP) tiene su funcionalidad y aplicabilidad radican en establecer y mantener los requisitos de seguridad en las distintas fases del desarrollo del software, permitiendo mitigar efectivamente los riesgos asociados a cada una, con esto se logra una reutilización de requisitos, amenazas, test y posibles soluciones a las brechas de seguridad que podamos encontrar en cada fase de desarrollo, de igual forma al ser una metodología que se implementa durante cada fase de desarrollo sus requisitos de seguridad, las amenazas y las soluciones van evolucionando durante el ciclo de vida del software hasta llegar al usuario final, logrando asi entregar un producto con altos estándares de seguridad.

RECOMENDACIONES

- Buscar estrategias de comunicación determinadas para el conocimiento de la monografía y en las ventajas que se les abren a las personas y a las empresas que puedan hacer uso de cada una de las recomendaciones.

- La falta de cultura hacia la lectura lleva a cabo el ocasional fracaso hacia las recomendaciones dadas en la presente monografía, por lo cual es necesario hacer una traducción al audio libro de la misma, esto permitirá llegar a muchas más personas que no tienen como costumbre la lectura.

- Hacer expansiva capacitación a las empresas, escuelas, universidades, micro empresarios, emprendedores, empresas del sector de redes sociales, en la necesidad del conocimiento de este trabajo, ya que por medio de este encontraran beneficios hacia su labor diaria de manejo de información.

BIBLIOGRAFIA

- Elsevier Digital Press. (2006). Securing HP NonStop servers in an open systems world. {Burlington, Mass.} .
- Firtman, S. (2005). Seguridad informática. Buenos Aires: MP Ediciones.
- González Cussac, J. (2000). Nuevas amenazas a la seguridad nacional. Editorial Tirant Lo Blanch.
- Howard, M., Leblanc, D., & Viega, J. (2006). 19 puntos críticos sobre seguridad de software. México: McGraw Hill.
- Leeuw, K., & Bergstra, J. (2007). The history of information security. Amsterdam: Elsevier.
- Okada, M. (2003). Software security. Berlin: Springer.
- Rivera, L. (2011). Tecnologías de la información I. McGraw-Hill Interamericana.
- Unión Internacional de Telecomunicaciones, Comisión Interamericana de Telecomunicaciones. Organización de Estados Americanos. (2005). Políticas de telecomunicaciones para las Américas. {Geneva, Switzerland} .
- Universitat Politécnica de Catalunya. (2015). TestCase Definition Software.

WEBGRAFÍA

- Berzal, Fernando., 2019. “El ciclo de vida de un sistema de información” {En línea} {2 Noviembre de 2018} disponible en: (http://elvex.ugr.es/idbis/db/docs/lifecycle.pdf

- Ecured.cu. 2016. Criptoanálisis - Ecured. {En línea} disponible en:(https://www.ecured.cu/Criptoan%C3%A1lisis) { 21 Diciembre 2018} .

- Es.wikipedia.org. 2018. Confidencialidad. {En línea} disponible en:(https://es.wikipedia.org/wiki/Confidencialidad) { 15 noviembre 2018}

- Es.wikipedia.org. 2016. *Cortafuegos (Informática)*. {En línea} disponible en:(https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)) {11 noviembre 2018}.

- Es.wikipedia.org. 2011. *Espionaje*. {En línea} disponible en:(https://es.wikipedia.org/wiki/Espionaje) {13 noviembre 2018}.

- Gestión de Riesgo en la Seguridad Informática, facilitando el manejo seguro de la información en organizaciones sociales, disponible en

  https://protejete.wordpress.com/gdr_principal/definicion_si/
  https://www.ecured.cu/Seguridad_Inform%C3%A1tica
  http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=2

- Gilbert Castro, A.A. 2014 “Guía para desarrollo de software seguro. {En línea}{2 Noviembre de 2018} disponible en:(https://es.slideshare.net/jesws1/guia-para-desarrollo-de-software-seguro)

- Gobierno, C., 2020. Decreto Ley Nº 199. Nov/99: Sobre La Seguridad Y Protección De La Información Estatal | SITEAL/TIC. {En línea} {2 noviembre de 2018} disponible en:(http://www.tic.siteal.iipe.unesco.org/normativa/1436/decreto-ley-no-199-nov99-sobre-la-seguridad-y-proteccion-de-la-informacion-estatal)

- Gonzalez, A., 2012. Control Interno En La Auditoría De Sistemas. {En línea} Es.slideshare.net. disponible en:(https://es.slideshare.net/AnaJulietaGonzlezGarca/control-interno-en-la-auditora-de-sistemas) {10 diciembre 2018}.

- Isecauditors.com. 2018. *Informática Forense Y Peritajes | Internet Security Auditors*. {En línea} disponible en:(https://www.isecauditors.com/informatica-forense-peritajes) {5 noviembre 2018}.

- Jaramillo, A., 2014. Modulo2 AUDITORIA INFORMATICA. {En línea} Es.slideshare.net. disponible en:(es.slideshare.net/anabeljaramillo526/modulo2-auditoria-informatica) { 21 noviembre 2018}.

- Julián, G., 2016. ¿Qué Es Un Ataque Ddos Y Cómo Pararlo?. {En línea} Genbeta.com. disponible en:(https://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta) { 26 Diciembre 2018} .

- López Provencio, Ferran. (2015). Metodologías para el desarrollo de software seguro. (tesis de pregrado). Recuperado de http://upcommons.upc.edu/bitstream/handle/2099.1/24902/103275.pdf?sequence=1

- MAGERIT: versión 1.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Guía para responsables del dominio protegible. V, Volumen 5
  Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996
  https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

- Mendoza, M., 2018. *ESET: Máximo Histórico De Vulnerabilidades Durante El 2017 @Esetla*. {En línea} Passion Points Mexico, disponible en:(https://passionpointsmx.wordpress.com/2018/01/15/eset-maximo-historico-de-vulnerabilidades-durante-el-2017-esetla/) {3 Noviembre 2018}.

- Moreno, J., 2017. *DEFENSA EN PROFUNDIDAD*. {En línea} Polux.unipiloto.edu.co. disponible en:(http://polux.unipiloto.edu.co:8080/00001345.pdf) {30 diciembre 2018}.

- Quesada, C., n.d. Mecanismos De Seguridad. {En línea} Profesores.fi-b.unam.mx. disponible en: (http://profesores.fi-b.unam.mx/cintia/Mecanismos.pdf) {10 noviembre 2018}

- Rimac, A., 2011. Auditoría De Sistemas Controles. {En línea} Es.slideshare.net. disponible en:(https://es.slideshare.net/villarrealino/auditora-de-sistemas-controles) {20 noviembre 2018}

❖ Villalón Huerta Antonio, SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN, 2007. disponible en: http://www.shutdown.es/seguridad.pdf

RESUMEN ANALÍTICO EN EDUCACIÓN – RAE

Información General	
1. Título	EL DESARROLLO DE UN SOFTWARE SEGURO LA MEJOR OPCIÓN PARA PROTEGER LA INFORMACIÓN
2. Autor	Anward Armando Acosta Piñeros
3. Edición	1ra
4. Fecha	27 Mayo 2020
5. Palabras clave	Seguridad, Herramientas, Sistema Operativo, So, Linux, Windows, Mac, Estrategia, Instalación, Métodos, Monitoreo, Información, Aplicación, Antivirus, Transacciones, Beneficios, Sociedad, Plagio, Privacidad, Tecnología.

6. Descripción.
El presente documento hace un recorrido por los conceptos generales que existen en la informática en relación a la seguridad informática, así mismo abarca problemas que se evidencian en el desconocimiento que pueda tener un usuario sobre la seguridad informática y los beneficios que esta le puede traer a su diario vivir, en donde se encuentra detallado, como un usuario con un poco de conocimiento, puede aplicar la seguridad informática en cualquiera de sus dispositivos de uso cotidiano. Se abarcará, como la metodología Security Requirements Engineering Process, nos puede ayudar a entregar un mejor producto a los usuarios finales.

7. Resumen.
Hoy en día la tecnología es un componente necesario para cualquier estructura sin importar el sector, siendo la encargada de emplear de una manera apropiada la seguridad digital, diseñando normas, técnicas y procedimientos, logrando mantener condiciones seguras durante el procesamiento de datos. Debido a esto se debe tener en cuenta tomar las determinaciones y órdenes (necesarias) ineludibles en cualquier sitio laboral previamente se pueda provocar un suceso de infalibilidad de los datos, como lo sería una fuga de la misma.
8. Planteamiento Del Problema
¿En qué se beneficia una sociedad de la protección Informática?
9. Objetivo General
Desarrollar una indagación que permita establecer la importancia del desarrollo de software seguro mediante la Metodología Security Requirements Engineering Process y cuál es su impacto positivo para la sociedad.
10. Objetivos Específicos
❖ Indagar cuáles son los riesgos y amenazas más frecuentes en el progreso del software seguro y como pueden evitarse.

❖ Establecer cuáles son las etapas del proceder del software seguro que puedan ser implementados para el desarrollo de un programa de software.

❖ Hacer un análisis de la metodología Security Requirements Engineering Process que permita conocer su funcionalidad y aplicabilidad para el desarrollo de un software seguro.

11. Marco Conceptual Y Teórico

MARCO CONCEPTUAL

Todas las estructuras informáticas deben dedicarse al desarrollo de la seguridad en y durante el intercambio de información, en el cual se dispone una comunicación continua, segura y con posibles periodos de inseguridad, con esto logramos establecer una utilidad en donde poseer datos es obtener el dominio de la información. Los riesgos, se deben intervenir de una manera preventiva, con el fin de proteger la privacidad, determinar los permisos de los usuarios por un nivel de confianza, al conceder esto se logra asegurar cada modelo o fase con el fin de garantizar un desarrollo seguro.

MARCO TEÓRICO

Almacenamiento documental. Se debe tener presente que el objetivo general de los medios de almacenamiento documental va desde la conservación, preservación, seguridad y consulta ágil y eficaz de los escritos primordiales, inclusive la reducción de la capacidad física o electrónica sin daño de los respectivos datos.

Concepto de almacenamiento documental. El almacenamiento documental lo podemos identificar como la implementación de una serie de procedimientos técnicos y lógicos que garanticen la protección, preservación y conservación de la información empresarial, soportados en medios técnicos universalmente aceptados, entre los cuales podemos citar los siguientes: archivos físicos organizados, micro-filmación, memorias USB, CD, DVD, discos duros y, más recientemente, en "La nube" almacenamiento virtual.

Medios de almacenamiento documental. Las técnicas de almacenamiento documental son variadas y las alternativas aumentan en la medida que avanzan los desarrollos tecnológicos.

12. Metodología

Para llevar a cabo este trabajo se tomó como base los conocimientos básicos o empíricos que posee una persona sobre que es la seguridad informática y en que le puede ayudar en su diario vivir, en muchos casos, las personas conocen lo básico o a veces nada sobre los beneficios de la seguridad informática y el resguardo de la información personal mientras se está en un dispositivo tecnológico. Al igual se tomaron varios escritos en referencia a la investigación para ser analizadas.

13. Resultado.

Después de realizar la investigación se busca dejar un documento donde se contextualice las amenazas más comunes usadas por el ciberdelincuente a las cuales están expuestos los usuarios y así mismo las formas, técnicas o métodos más comunes que se están usando para evitar o ya en caso extremo de corregir estas amenazas en el ciberespacio, todo esto con el fin de preservar la información que se almacena en el sistema, así mismo se deja expresado de cuál sería la mejor alternativa que nos ayudaría en el desarrollo y posterior entregar de un Software seguro, esta Metodología es la Security Requirements Engineering Process la cual es la más adecuada y recomendada, dado que esta se basa en la aplicación de la seguridad informática en las distintas etapas del proceso de creación de software, cumpliendo de mejor forma con las necesidades que se podrían presentar.

14. Fuentes.

- Elsevier Digital Press. (2006). Securing HP NonStop servers in an open systems world. {Burlington, Mass.} .
- Firtman, S. (2005). Seguridad informática. Buenos Aires: MP Ediciones.
- González Cussac, J. (2000). Nuevas amenazas a la seguridad nacional. Editorial Tirant Lo Blanch.
- Howard, M., Leblanc, D., & Viega, J. (2006). 19 puntos críticos sobre seguridad de software. México: McGraw Hill.
- Leeuw, K., & Bergstra, J. (2007). The history of information security. Amsterdam: Elsevier.
- Okada, M. (2003). Software security. Berlin: Springer.
- Rivera, L. (2011). Tecnologías de la información I. McGraw-Hill Interamericana.
- Unión Internacional de Telecomunicaciones, Comisión Interamericana de Telecomunicaciones. Organización de Estados Americanos. (2005). Políticas de telecomunicaciones para las Américas. {Geneva, Switzerland} .
- Universitat Politécnica de Catalunya. (2015). TestCase Definition Software.

15. Contenidos.

Está dividido en tres capítulos: El primer capítulo analiza los riesgos y amenazas en el desarrollo del Software Seguro, la estructura que se va a llevar para la seguridad, la forma en que se deben proteger los datos, con esto se podría llegar a mitigar amenazas hasta el punto de llegar a disminuirlas, con esto se lograría un periodo vital en el desarrollo de software. El segundo capítulo analiza el Periodo vital de un software y su uso en su progreso de un programa de software. En donde se nombran los ciclos vitales de software los cuales son conjuntos usados y empleados en la sociedad durante el progreso del software, con el fin de diseñar servicios en cualquier plataforma y de cualquier índole, logrando así que sean convincentes y aceptables en el momento de emprender el desarrollo de software. El capítulo tercero analiza la Metodología Security Requirements Engineering Process su funcionalidad y aplicabilidad para el desarrollo de software también conocida como SREP, la cual es un proceso que se basa en activos y dirigido para la creación de requerimientos de protección en el proceso de un Sistema de Información Seguro, esta metodología es la herramienta de Common Criteria “CC”, donde el “CC” es un estándar internacional ISO/IEC 15408 el cual habla sobre seguridad informática en las distintas etapas del proceso de creación de software, donde su meta es determinar los requerimientos que sean necesario a los diseñadores del software determinar los rasgos de garantía y así mismo poder estimar sus resultados efectuar su objetivo. Esta metodología describe como integrar los periodos vitales de un Software Seguro en su etapa de progreso cerca con la utilización repositorios para la protección facilitando la reutilización de requisitos, activos o bienes, amenazas y soluciones a un error planteado.

16. Conclusiones.

En esta investigación se le dio luces a nuestra sociedad de cómo puede llevar a cabo la protección de sus datos, como también a conocer cada método existente, las amenazas a las cuales nos encontramos expuestos a diario cuando usamos las redes, así como también de que es lo que se debe proteger cada una de las personas para no ser perjudicados con su información y exponerse a que se haga un mal uso de las mismas.

Se dejó claro sobre los distintos riesgos y las amenazas que existen para el software, los cuales van desde los desastres naturales, pasando por personal cercano al desarrollo el proyecto, los cuales pueden sustraer o sabotear información debido a algún mal entendido o por diferencias con el personal, así como personal que no tiene nada que ver con el desarrollo sino que pasan su vida haciendo daño de forma remota o con la creación de programas los cuales afectan o sustraen información precisa, dentro de estos programas dejamos en evidencia los más comunes en nuestro diario vivir, así como los nombres de las técnicas que los ciber delincuentes usan para implantar estos programas, las cuales van desde enviar un email el cual contiene una dirección la cual al abrir descargara el programa malicioso y se ejecutara sin que el usuario final tenga conocimiento de que es víctima de un ciberataque.

Afortunadamente para estas amenazas existen en el mercado software y hardware (Antivirus, Firewall, Antimalware, Antispyware), los cuales nos brindan soluciones completas, aunque muchas de las soluciones que nos brindan estos programas las podemos encontrar en nosotros mismo como primera barrera ante un ataque, dado que somos nosotros los que inconscientemente ejecutamos, abrimos o ingresamos a sitios de dudosa reputación, dejamos nuestros equipos sin clave para el ingreso al sistema en donde esta debe ser una de las primeras medidas para evitar que usuarios o personal ajeno al uso de nuestro equipo ingrese y pueda ejecutar ya sea inconscientemente o con uso de razón programas que causaran daños a nuestra información.