Protocolo para la implementación de buenas prácticas de Seguridad Informática y de la Información para los usuarios en la Universidad del Valle

AUTOR
Jhon Jairo Pantoja

Universidad Del Valle
Escuela De Ingeniería De Sistemas Y Computación
Ingeniería de Sistemas
Santiago De Cali, Valle Del Cauca
Junio 2017

Protocolo para la implementación de buenas prácticas de Seguridad Informática y de la Información para los usuarios en la Universidad del Valle

AUTOR
Jhon Jairo Pantoja

Como requisito parcial
para la obtención del título:
Ingeniero De Sistemas

DIRECTOR
John Alexander Sanabria

Universidad Del Valle
Escuela De Ingeniería De Sistemas Y Computación
Ingeniería de Sistemas
Santiago De Cali, Valle Del Cauca
Junio 2017

Resumen

En el presente trabajo de grado se diseñó y planteó un protocolo para la implementación de buenas prácticas de seguridad informática y de la información en la Universidad del Valle, con el fin de promover mejores acciones para la formación en ciberseguridad a los miembros de la organización, que beneficien la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas y operaciones, y la adaptación de las políticas de seguridad establecidas por la institución[1]. Como resultado se esbozan debilidades encontradas y se emiten recomendaciones que contribuyan a mejorar su nivel de seguridad.

Hay escasa información y manejo de esta temática en un gran porcentaje de organizaciones, principalmente en las educativas, así como lo plantea Foursys, en el top cinco de los errores en materia de *ciberseguridad* cometidos en la educación[2]. Tiene mucha importancia suplir de medios o buenas prácticas a todos los miembros de la institución, para así poder controlar todo tipo de riesgos que puedan presentarse en cada uno de los procesos adyacentes. La universidad carece de un sistema o algún protocolo que sirva de guía a los miembros de la organización, para brindarles una mejor orientación en la elección y uso de herramientas informáticas.

Así pues, el propósito de plantear este protocolo es sensibilizar una cultura de seguridad en la organización exponiendo unas vulnerabilidades de la universidad, para incentivar la protección de los activos de información (véase Capítulo 6.3.6.4); para conseguir confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada usuario que este relacionado con las tecnologías informáticas.

Contenido

Lista de figuras

Lista de tablas

Agradecimientos

Agradezco,

A Dios por nutrir mi fe en mi formación académica y personal, a mis padres, familiares y a mi novia, por su apoyo y comprensión en la elaboración de este trabajo de grado, al profesor John Alexander Sanabria por su atenta dirección en el desarrollo del proyecto, a Pablo Emilio Astroz por su colaboración, a Hugo Bayona por su instrucción y disponibilidad para mi formación en el área de seguridad informática, al profesor Miguel José Navas por su disponibilidad y recomendaciones en la elaboración del proyecto, y a mis compañeros de la universidad por su constante motivación en el desarrollo de este trabajo, de antemano,
gracias.

Introducción

Actualmente, la seguridad informática está en auge, como lo demuestra la inversión de recursos que empiezan a realizar entidades gubernamentales en materia de ciberseguridad, como el Reino Unido [9], donde también muestran el aumento de amenazas. Las brechas de seguridad aumentan a medida que se evidencia la evolución de las plataformas computacionales, que tienen sus raíces desde la creación de la primer computadora hasta las supercomputadoras usadas hoy en día[10]. El recurso más importante de una empresa es la información, la cual está soportada por estas tecnologías que permiten su almacenamiento y procesamiento; más importante aún, es considerar la importancia de brindar una buena protección que debe ser conocida por las personas encargadas de operar con ella.

No obstante, muchas organizaciones han optado por abordar directrices que orienten el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera, promover unas buenas prácticas de seguridad informática y de la información, sirve de herramienta para concienciar a los miembros de la entidad sobre la importancia y sensibilidad de la información.

La universidad como organización educativa igualmente trata con grandes volúmenes de información. Es necesario llevar a cabo dentro de sus procesos, buenas prácticas que permitan brindar una mayor seguridad. Tanto como es importante incentivar y divulgar apropiadamente estas buenas prácticas en pro de la seguridad informática y de la información de la institución. Se lleva a cabo la construcción de un protocolo, que a través de sus pasos, intenta promover una mejor cultura de ciberseguridad para la universidad; teniendo en cuenta la adopción de normas ISO/IEC 27001[7] y consideraciones de seguridad informática tomadas de grandes empresas e instituciones educativas.

1 Descripción del problema

1.1 Planteamiento del problema

Históricamente, en los años 60, la finalidad de los primeros *hackers* era explorar el potencial de las comunicaciones en red y los recursos compartidos, es decir, la información [11]. Después de los 60, software de bases de datos fueron impuestos para permitir compartir datos al interior de una empresa u organización, luego esos centros de datos que mantenían aislados se hicieron accesibles a todo el mundo con la llegada del internet. Con ello vino la Web, las redes de contenidos. La siguiente etapa corresponde al desarrollo de redes sociales, las redes de personas, basadas en compartir información personal, la comunicación, construcción de comunidades; el usuario pasa de ser un simple consumidor a ser un productor de información [12]. Con el predominio del internet de las cosas (IoT), redes de transmisión y redes sociales, el *big data* es generado en cada segundo que pasa. Estos grandes volúmenes de información dictaminan la importancia de la seguridad de la información; ya que se han convertido en objetivo de ciberataques y es necesario brindar una adecuada seguridad a los datos [13].

Existen variedad de técnicas que un atacante usa para sacar provecho de los riesgos a los que se exponen las tecnologías de información. El sitio web Hackmageddon del autor Paolo Passeri[3] realiza constantes reportes sobre ciberseguridad. Uno realizado en Febrero del 2017, en la Fig. 1.1.1, se observa que los ataques en su mayoría son por delitos informáticos.

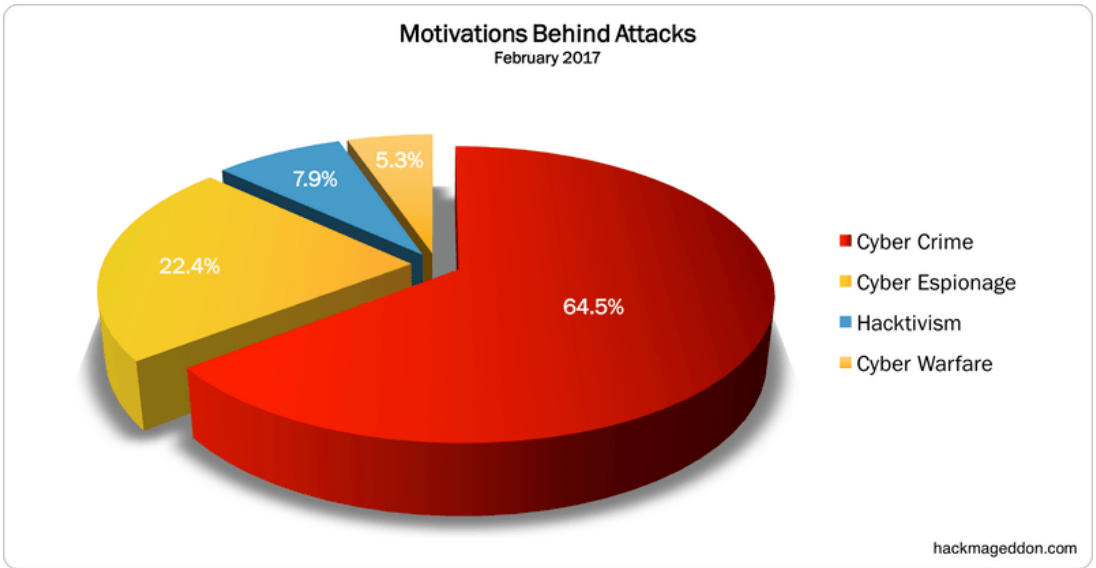

Figure 1.1.1: Motivación detrás de los ataques. (Imagen tomada de [3])

Los otros motivos de ataques corresponden al *Hacktivismo*, *Ciberespionaje* y *Ciberguerra* que igualmente buscan explotar las vulnerabilidades presentes en las tecnologías de información en distintos campos, como el político.

Las diferentes técnicas de ataques reportadas en el 2017 se pueden ver en la Fig 1.1.2, y entre las más conocidas están:

- Inyección *SQL*
- Ataque dirigido
- *Defacement*
- Denegación de servicios
- Robo de cuentas
- *Malvertising*
- *Malware*

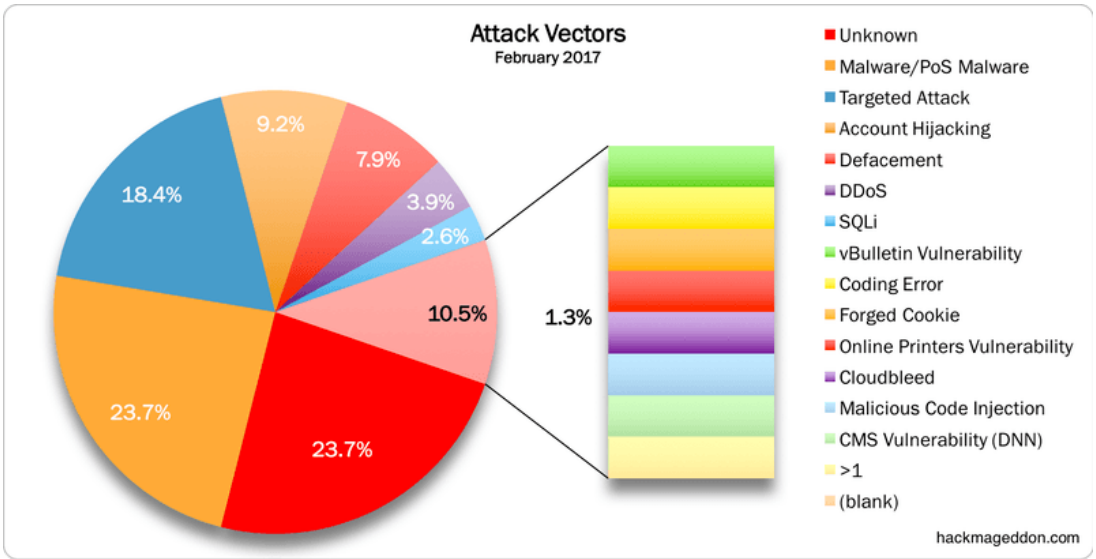

Figure 1.1.2: Tipos de ataques. (Imagen tomada de [3])

Existen prácticas de seguridad informática comunes y generales que toda organización debería acoger, como las brindadas por la IIROC(Investment Industry Regulatory Organization of Canada)[14]:

- Identificar qué activos necesitan asegurarse, así como las amenazas y los riesgos para ellos.
- Proteger los activos con los adecuados mecanismos de protección.
- Detectar intrusiones, brechas y accesos no autorizados.
- Responder a un posible evento de ciberseguridad (o seguridad informática).
- Recuperación de un evento de ciberseguridad restableciendo operaciones y servicios a la normalidad.

Para la acogida de buenas prácticas de seguridad, es necesario que se agreguen mecanismos como la instauración de políticas que regulen el cumplimiento de los objetivos propuestos para asegurar la información de la organización, o que se lleven a cabo programas de concienciación sobre la importancia de la seguridad informática y de la información [15]. Pues, la mayoría de las fallas de seguridad surgen como resultado de factores humanos y organizativos, una administración deficiente, un uso indebido de los sistemas de información por parte de los miembros de la organización, un incumplimiento de la política de seguridad de la información y la falta de una estrategia de seguridad de la información organizacional. Las cuales han demostrado ser causantes, directa e indirectamente, del aumento de fallas de seguridad de la información[16].

Symantec es una corporación internacional que desarrolla y comercializa software para computadoras, particularmente en el dominio de la seguridad informática. Recolecta información de ataques de 98 millones de sensores de ataques en el mundo, además monitorea amenazas en más de 157 países a

través de la combinación de productos Symantec, tecnologías y servicios, entre otras terceras partes que permiten la extracción de datos, como Norton [4]. Dentro del último reporte en la Fig. 1.1.3 tenemos la clasificación de los sitios web más vulnerados por categoría, resultado del constante análisis de la *honeypot* de Symantec; se puede ver que el sector educativo hace parte del top 10 y que tuvo un incremento porcentual afectado del 2015 al 2016 [4].

Rank	Domain Categories	2015 (%)	2016 (%)	Percentage Point Difference
1	Technology	23.2	20.7	-2.5
2	Business	8.1	11.3	3.2
3	Blogging	7.0	8.6	1.6
4	Hosting	0.6	7.2	6.6
5	Health	1.9	5.7	3.8
6	Shopping	2.4	4.2	1.8
7	Educational	4.0	4.1	< 0.1
8	Entertainment	2.6	4.0	1.4
9	Travel	1.5	3.6	2.1
10	Gambling	0.6	2.8	2.2

Figure 1.1.3: Sitios web más atacados por categoría. (Imagen tomada de [4])

Las TI como miembro integral del entorno de las universidades, atribuyen de igual manera que la información es uno de los activos más prominentes y debe protegerse de la violación de la seguridad. Estas entidades educativas están a la vanguardia de los avances tecnológicos. Dichas tecnologías permiten un entorno de aprendizaje valioso, pero por otro lado lo vuelven más vulnerable [17]. La medición de los riesgos de seguridad puede ser evaluada en estas categorías: exposición de contraseñas, ingeniería social, reputación de direcciones *IP*, instalación de parches de seguridad, entre otros; así lo destaca un reporte hecho por SecurityScorecard a 485 colegios y universidades [18]. Uno de los casos de estudio de vulnerabilidades de la Universidad del Valle expuesto más adelante en el trabajo de grado, detalla el riesgo al que se expone un sistema de información en materia de exposición de contraseñas.

1.2 Formulación del problema

Los distintos problemas que la violación de la seguridad informática conlleva, provienen del poco conocimiento que se tiene acerca del manejo seguro de las TI en las distintas organizaciones, al igual que la no promulgación de la importancia de la seguridad informática en la actualidad. Según el reporte de Symantec, el sector educativo tiene un índice no muy alto de ataques a sus sitios web, comparado con los sectores tecnológicos[4]. Sin embargo, esto no las excluye de llegar a ser víctimas en conjunto con otras organizaciones de mayor tamaño y recibir cualquier tipo de ataque, ya sea de poca

o gran magnitud, como se termino viendo el alcance del popular y reciente ataque del ransomware que tocó sectores y compañías que no habían presenciado algo semejante anteriormente, dicho ataque tiene la finalidad de hacerse el control de los equipos objetivos, encriptar la información y solicitar un pago para su debido rescate[19].

La educación en seguridad informática y de la información es necesaria para generar consciencia en el uso de buenas prácticas de seguridad en las organizaciones educativas, teniendo en cuenta que en casi todos los sectores se hace uso de sistemas de computo y redes [20]. Tanto es necesario que los usuarios comunes sean capacitados, como por otro lado los usuarios del área de tecnologías de la información son quienes desarrollarán las tecnologías de información del futuro y se les debe brindar un entrenamiento adecuado[21]. Entre las fallas más comunes en las universidades en materia de seguridad informática según Foursys[2], compañía que suple soluciones de seguridad al sector educativo, están:

- Débil filtrado en los sitios web.
- Mala visibilidad y control de la red.
- No instalar parches de seguridad a aplicaciones No-Microsoft.
- Falta de encriptado de datos.
- No educación a los usuarios frente a la importancia de la seguridad informática y de la información.

Como lo demuestra una reciente noticia, una universidad de Londres, la University College London, fue víctima también de un ransomware; siendo esta universidad un ”centro de excelencia en la investigación cibernética”, estatus otorgado por el servicio de inteligencia y monitoreo del GCHQ(Government Communications Headquarters). ”Los piratas informáticos tienden a apuntar a la gente que estará desesperada para conseguir el acceso a sus datos y es, por lo tanto, los más probables de que paguen el rescate”.”En la actualidad hay un montón de estudiantes que van a poner los toques finales a sus disertaciones, por lo que podría ser que fueron los objetivos”[22].

Dado esto, entonces: ¿Cómo debe diseñarse una guía para incentivar buenas prácticas de la seguridad informática y de la información en la Universidad del Valle?

2 Justificación

2.1 Justificación económica

Uno de los factores más importantes en los problemas que frente a seguridad cibernética se refiere, son los activos informáticos. Minimizar la escala de riesgos en la organización implica una reducción de daños en estos activos (véase Capítulo 5.3.6), que a su vez representan diferentes valores en materia de recursos de la Universidad.

2.2 Justificación social

Toda organización actualmente posee y maneja información, detrás de la cual esta la otra parte importante y son las personas encargadas. Mitigar las vulnerabilidades a las que pueden ser expuestos, permite que el impacto sea mucho menor, puesto que en su gran mayoría los ataques tienen como primer objetivo encontrar huecos de seguridad en los usuarios internos o los externos que tengan relación con la empresa.

2.3 Justificación académica

Teniendo en cuenta que la Universidad del Valle es una organización, educativa en este caso, tener consigo una guía en el ámbito de la seguridad informática y de la información, genera conciencia a los miembros de la institución universitaria, sobre los riesgos que pueden llegar a alcanzarse si no se tuviese una

adecuada manera de aminorarlos. De esta forma la entidad educativa necesita llevar una buena formación en este aspecto, para beneficio propio como empresa y para con las entidades que acojan sus estudiantes para una posición laboral.

3
Objetivos

3.0.1 Objetivo General

Elaborar un protocolo que permita la implementación de buenas prácticas de seguridad informática y de la información para los usuarios relacionados con el área de TI en la Universidad del Valle.

3.0.2 Objetivos Específicos

1. Indagar acerca de la seguridad informática y de la información.
2. Indagar sobre protocolos.
3. Clasificar la información y aplicaciones utilizadas en todas las áreas que tengan uso de TI en la universidad.
4. Indagar sobre las normas ISO que sirven de metodologías para la seguridad informática.
5. Esbozar las vulnerabilidades más frecuentes en los sistemas informáticos de la Universidad.
6. Validar el protocolo realizando un estudio de comparación de los procesos con y sin éste.

4

Tabla de Resultados

Objetivo	**Resultado**
Indagar acerca de la seguridad informática y de la información.	Capítulo 6.3.1, 6.3.2, 6.3.3 y 6.3.4.
Indagar sobre protocolos.	Para este objetivo la finalidad es estudiar la terminología de ”protocolos” alusiva a la informática, junto con sus estructuras y procedimientos, Capítulo 6.3.5.
Clasificar la información y aplicaciones utilizadas en todas las áreas que tengan uso de TI en la universidad.	Capítulo 7.1.
Indagar sobre las normas ISO que sirven de metodologías para la seguridad informática.	Capítulo 6.3.6.
Esbozar las vulnerabilidades más frecuentes en los sistemas informáticos de la Universidad.	Capítulo 9.3.
Validar el protocolo realizando un estudio de comparación de los procesos con y sin éste.	Capítulo 9.3.

Table 4.0.1: Objetivos específicos frente a resultados obtenidos.

5
Alcance

La elaboración del proyecto se desarrollará en la Universidad del Valle, inicialmente en el área de la OITEL (Oficina de Informática y Telecomunicaciones), pasando a objetos de estudio como lo son las partes tanto administrativa y la educativa; se es necesario acudir a investigar las áreas en las que esté presente TI para tener un mejor análisis, en la escuela de ingeniería de sistemas y la facultad de salud, de las que se estudiará los sistemas de información principales manejados por los administradores de sistemas encargados de cada escuela. Los usuarios que pueden hacer uso del protocolo son aquellos que tengan conocimientos básicos en informática o que tengan constante labor con tecnologías informáticas como computadores personales propios o de la universidad, y tanto dispositivos celulares, que manipulen información de la universidad o personal tanto de carácter pública como confidencial. El suministro de información estará limitado, debido a la restricción de confidencialidad de la información estipulada por la oficina de informática; es decir estará ligado a obtener información superficial sobre datos personales y manejo de información por parte de los administradores de sistemas a los que sea posible entrevistar.

6
Marco Referencial

6.1 Glosario

A

Ataque dirigido: Es cualquier tipo de ataque malicioso que tiene como objetivo un individuo específico, compañía, sistema o software. Puede ser usado para extraer información, perturbar operaciones, infectar máquinas o destruir un tipo de datos específico en una máquina destino [23].

B

Backups: Es una copia de datos realizada como medida de seguridad para evitar la pérdida de estos [7].

C

Ciberespionaje: es aquel acto con el cual se obtienen secretos sin el permiso de aquél quien es dueño de la información. Se puede considerar como objetivo de ciberespionaje toda aquella información personal, clasificada, de propiedad o de sentido delicado y puede ser pertenencia de individuos, competidores, grupos, rivales y gobiernos [24].

Ciberguerra o guerra cibernética: es un conflicto basado en Internet que involucra ataques de motivación política a información y sistemas de información información. Los ataques de ciberguerra

pueden desactivar los sitios web y las redes oficiales, interrumpir o inhabilitar los servicios esenciales, robar o alterar los datos clasificados, y alterar los sistemas financieros - entre muchas otras posibilidades[25].

D

Defacement: Es un tipo de ataque informático en el que el atacante irrumpe en el servidor web y reemplaza el sitio hosteado por otro de su autoría, utilizando técnicas como el phishing, la inyección de código, el cross site scripting, entre otros [26].

Denegación de servicios DDoS: es un intento de hacer que un servicio en línea no esté disponible al sobrecargarlo con el tráfico de múltiples fuentes. Múltiples sistemas informáticos comprometidos atacan un objetivo, como un servidor, un sitio web u otro recurso de red, y provocan una denegación de servicio para los usuarios que estén usando el recurso [27].

DHCP (Dynamic Host Configuration Protocol): Protocolo de configuración dinámica de host, es un protocolo de administración de red utilizado para asignar dinámicamente una dirección IP a cualquier nuevo nodo que ingrese a la red [28].

DNS (Domain Name System): es un servidor que contiene una base de datos de direcciones IP públicas y sus nombres de host asociados; y en la mayoría de los casos, sirve para resolver, o traducir, esos nombres comunes a las direcciones IP según lo solicitado [29].

E

Ethical hacking o Hacking Ético: Se refiere al procedimiento llevado a cabo por una o varias personas que usan sus conocimientos de seguridad informática para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño[30].

F

Firewalls: Programas informáticos que controlan el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad [31].

H

Hacker: Persona que utiliza los ordenadores como reto intelectual, con amplios conocimientos informáticos [32].

Hacktivismo:(un acrónimo de hacker y activismo) se entiende normalmente "la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramien-

tas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software"[33].

Honeypot: Es típicamente un computador, red o sistema de datos que parece ser parte de un gran sistema, pero es un vehículo controlado, independiente, que hace la función de "señuelo" para atraer a aquellos que quieren infectar o abusar del sistema; monitorizando así estos ataques para que no afecten el sistema que está siendo protegido[34].

I

Ingeniería social: El arte de utilizar las personas como medio para atacar los sistemas informáticos [35].

Inyección SQL: Es un tipo de ataque de código informático que permite hacerse el control de la base de datos de un sistema [36].

M

Malvertising: Hace referencia a un tipo de ataque informático que infecta un objetivo a través de publicidades en sitios web [37]. Malware: Es un término general que se le da a todo aquel software que perjudica a la computadora. La palabra malware proviene del término en inglés malicious software, y en español es conocido con el nombre de código malicioso [38].

O

Open Source: Open source se refiere a cualquier programa de software cuyo código fuente esté disponible para uso, modificación y redistribución a cualquier usuario [39].

P

Protocolo: Es el término que se emplea para denominar al conjunto de normas, reglas y pautas que sirven para guiar una conducta o acción [40].

S

SGSI: Es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información [41].

T

TI: Se refiere a todo lo relacionado con las tecnologías computacionales o informáticas, desde las redes, el hardware, el software, hasta las personas que trabajan con las tecnologías de la información [42].

TIC: Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes [43].

V

Virus informático: Es un programa malicioso que se introduce en un ordenador, sin permiso o sin conocimiento de su usuario, para alterar su funcionamiento y, particularmente, con la finalidad de modificar o dañar el sistema [44].

6.2 Antecedentes

Las políticas y prácticas de seguridad informática dentro de las organizaciones en su gran mayoría son regidas e implementadas a través de normas o estándares como lo son las ISO 27000, cuya autoría está regida por la BSI (British Standard Institution), entidades normalizadoras británicas. El origen del estándar proviene de ideas como la de crear un criterio de evaluación de la seguridad para los productos TI de seguridad del gobierno del Reino Unido en el departamento DTI (Department of Trade and Industry)[45]. De éste se desplegaron otros estándares relacionados, conformando así una a una la familia o series de la ISO 27000, concebida y anunciada en 2005. Tienen como principal objetivo definir requisitos para un SGSI (Sistema de Gestión de la Seguridad de la Información). Es altamente recomendado para todo tipo de empresas grandes o pequeñas, especialmente para sectores que operan con información crítica o manejo de información de otras entidades.

Muchas de las entidades cuentan con proyectos de seguridad de la información pero muy pocas tienen sus procesos certificados por la ISO/IEC 27001 [46], la cual permite tratar los riesgos presentes en aspectos relacionados a la disponibilidad, confidencialidad e integridad de la información; y tener dicha certificación implica adaptarse a las prácticas de seguridad mundialmente aceptadas.

En una encuesta global del 2016 sobre la certificación de la ISO/IEC 27001 en las empresas grandes y pequeñas, realizada a 53 países, se concluyó que la mayoría de las organizaciones participantes optan este estándar para mejorar la seguridad de la información.[47]

A nivel internacional muchas de las grandes organizaciones educativas poseen sus políticas de seguridad para implementar las mejores prácticas para proteger la información; además de folletos informativos de seguridad informática en los campus, y recomendaciones de seguridad dispuestas a los usuarios de la comunidad.

A continuación se destacan ciertas políticas de seguridad que poseen diferentes Universidades, entre ellas:

- Ryerson University [48].
- Harvard University [49].
- McGill University [50].

6.2.1 Ryerson University - Toronto, Canadá.

Directrices de acceso

Información pública: La información contenida en la universidad en su mayoría es de carácter público, por ejemplo: el directorio telefónico, calendarios, horarios, libros generales de la biblioteca, varias reuniones, conferencias y boletines informativos. Información restringida: Al 10 de junio de 2006, la Universidad quedó sujeta a la Ley de Protección de la Información y la Privacidad (FIPPA ó Freedom of Information and Protection of Privacy Act) que regula los requisitos legales relativos al uso, divulgación y retención de información personal, así como la obligación de proporcionar acceso a los registros de la universidad con protección limitada para ciertos tipos de información restringida (consulte la pestaña "privacidad" de la página WEB de Ryerson para la "Política de acceso y protección de información restringida (IPAP-RI)"). La información de carácter restringido o legalmente restringido, como la protegida por las leyes federales y provinciales sobre derechos y privacidad, sólo debe ser accesada por aquellos miembros autorizados de la comunidad universitaria con una necesidad específica y legítima. El acceso legítimo no incluye la libertad de buscar información más allá de lo específicamente requerido para realizar una tarea relacionada con el trabajo o una investigación autorizada.

Directrices de uso

1. Cada miembro de la comunidad Universitaria es responsable por el uso apropiado del activo de información en lo que respecta a su área de trabajo, a los términos de esta política y los procedimientos establecidos para este propósito.

2. El uso apropiado se define como el uso sabio y prudente de la información para que los recursos no se desperdicien, dañen o corrompan. El uso inapropiado incluye borrar, tomar o modificar la información sin la autorización apropiada, desfigurar o quitar páginas de libros, usar información para avergonzar, intimidar o acosar, o intentar subvertir el flujo de información, como intentar accidentalmente estrellar o ralentizar sistemas informáticos, modificar o eliminar la información publicada sin autorización, y otras acciones similares.

3. La investigación autorizada está definida por los límites a los que están sujetas las áreas de investigación.

Responsabilidades

Departamento o Facultad: Cada usuario de la facultad, responsable de la información de la Universidad deberá aumentar la probabilidad de que la información sea utilizada correcta y apropiadamente al:

1. Identificar que la información se mantenga.

2. Determinar si es de naturaleza restringida y/o altamente sensible a los riesgos.

3. Desarrollar, implementar y mantener procedimientos razonables y claros que:

- Establezcan reglas de acceso.
- Identifiquen los requisitos y responsabilidades de control de cambios.
- Identifiquen los requisitos de confidencialidad.
- Promuevan buenas prácticas, tales como bloquear archivos confidenciales cuando no se usan, destruir información confidencial cuando se descarta y no compartir contraseñas con cuentas de computadora con nadie más que su supervisor y / o el oficial de seguridad de información del departamento.
- Establezcan prácticas apropiadas de contraseña, integridad de datos, almacenamiento, copia de seguridad y recuperación donde existan aplicaciones informáticas de departamentos locales.

4. Que los empleados firmen un reconocimiento de que son conscientes de esta política y los procedimientos relacionados, y que se espera que actúen de manera apropiada para mantener la confidencialidad e integridad de la información a la que tienen acceso.

Propietario de aplicación: Más allá de las responsabilidades de los usuarios de la facultad, algunos departamentos también son ”propietarios” de aplicaciones informáticas. Ejemplos de estas aplicaciones incluyen Sistemas Financieros, Recursos Humanos / Sistemas de Nómina, Sistemas de Información para Estudiantes, Sistemas de Alumnos y diversos sistemas académicos.

La propiedad de estos sistemas incluye responsabilidades como:

1. Establecer normas de acceso a las solicitudes para la comunidad universitaria en general.

2. Desarrollar, implementar y mantener procedimientos razonables y claros para otorgar acceso a la solicitud de la comunidad universitaria en general.

3. Designar a un oficial de seguridad de aplicaciones dentro del departamento del ”propietario”, el cual es responsable de configurar y mantener perfiles de acceso de seguridad de usuarios autorizados en estos sistemas.

Mantener las habilidades necesarias para apoyar estas prácticas.

Técnico: Más allá de las responsabilidades de ”usuarios” y ”propiedad de aplicaciones”, algunos departamentos tienen la responsabilidad del procesamiento de tráfico (programas de computadora) y el almacenamiento de datos en nombre de la comunidad universitaria.

Estos departamentos tienen las responsabilidades adicionales de:

1. Establecer las reglas de acceso a la infraestructura técnica para la comunidad universitaria (acceso a redes y computadoras).

2. Establecer reglas de control de cambios para la tecnología de procesamiento y almacenamiento (programas informáticos y bases de datos).

3. Establecer reglas de almacenamiento, copia de seguridad y recuperación para programas informáticos y bases de datos.

4. Desarrollar, implementar y mantener procedimientos razonables y claros para otorgar acceso a la infraestructura técnica, almacenamiento, respaldo, integridad de datos y prácticas de recuperación.

5. Designar a un oficial de seguridad de datos dentro del departamento "técnico" responsable de establecer y mantener perfiles de acceso de seguridad de usuario autorizados para la infraestructura técnica.

6. Manteniendo las habilidades necesarias para apoyar estas prácticas.

Oficial de Seguridad de Sistemas de Información (ISSO - Information Systems Security Officer): La principal responsabilidad del ISSO es proteger la integridad del activo de la información en toda la comunidad universitaria. Lo cual se llevará a cabo:

1. Ayudando a todos los departamentos de la Universidad a desarrollar prácticas y procedimientos sólidos y coherentes en el sistema de información.

2. Trabajando con la aplicación y los oficiales de seguridad de datos para desarrollar:

- Las interfaces de seguridad necesarias entre los sistemas de aplicación y las infraestructuras técnicas.
- Reglas de control de cambios para las aplicaciones y actualizaciones de las bases de datos.
- Almacenamiento de datos, copia de seguridad, integridad de datos y requisitos de recuperación.

3. Investigando los últimos avances tecnológicos en software y prácticas de seguridad de la información y recomendando cambios y mejoras apropiados al entorno de los sistemas de información de la Universidad.

4. Monitoreando el entorno de los sistemas de información de la Universidad y la información de la administración y la auditoría interna de posibles infracciones de la seguridad, los procedimientos y/o la política.

Auditoría: : El departamento de Auditoría Interna incluirá, en sus actividades de auditoría departamentales, el cumplimiento de esta política y los procedimientos departamentales asociados.

6.2.2 Harvard University - Cambridge, Massachusetts, Estados Unidos

La política de seguridad de la información de la universidad de Harvard consta de tres aspectos: Declaraciones de la política, Requerimientos y el "How-To";que especifica la implementación que acompaña a los requerimientos.

Declaraciones de la política

La Universidad de Harvard se compromete a proteger la información que es crítica para la enseñanza, la investigación y la variedad de actividades de la Universidad, nuestra operación comercial y las comunidades que apoyamos, incluyendo estudiantes, profesores, miembros del personal y el público. Estas protecciones pueden regirse por consideraciones legales, contractuales o de la Universidad.

Todos en Harvard tienen la responsabilidad de manejar y proteger apropiadamente la información confidencial según lo establecido en las Declaraciones de la Política. Estas políticas se aplican a toda la comunidad de Harvard incluyendo profesores, personal y estudiantes. Cada política está respaldada por Requisitos que describen lo que se debe hacer para estar en cumplimiento. Los pasos específicos de implementación se describen en el How-To que acompaña a los Requisitos.

1. Todos los usuarios son responsables de proteger la información confidencial de Harvard que usen en cualquier forma del acceso y uso no autorizado.

2. Todos los usuarios son responsables de proteger sus contraseñas de Harvard y otras credenciales de acceso contra el uso no autorizado.

3. Todo acceso y uso de la información confidencial de Harvard debe ser para propósitos autorizados de Harvard.

4. Todo acceso a los sistemas que manejan la información confidencial de Harvard debe ser para propósitos autorizados de Harvard.

5. Todas las personas que accedan a la información confidencial de Harvard deben estar capacitadas para proteger dicha información.

6. Todos los usuarios de los recursos de información confidencial de Harvard deben identificarse de manera precisa e individual.

7. La información confidencial de Harvard debe estar protegida en cualquier computadora de usuario o dispositivo portátil.

8. Todos los servidores que almacenen información confidencial de Harvard deben estar protegidos contra el acceso inapropiado.

9. Todos los servidores y ubicaciones donde se almacena información de Nivel 4 o 5 deben estar identificados con exactitud y estar físicamente seguros.

10. Los registros electrónicos y físicos que contengan información confidencial de Harvard deben ser protegidos adecuadamente cuando se transportan o transmiten.

11. El software debe mantenerse actualizado en todos los ordenadores y dispositivos que procesan o almacenan información confidencial de Harvard.

12. Debe existir un mecanismo para limitar el número de intentos fallidos de iniciar sesión en una aplicación o servidor que procesa o almacena información confidencial de Harvard.

13. Los registros electrónicos y físicos que contengan información confidencial de Harvard deben ser eliminados adecuadamente para que la información no pueda ser recuperada o reensamblada cuando ya no sea necesario o no se requiera mantenerla.

14. Harvard debe llevar a cabo la debida diligencia apropiada para asegurar que los terceros que almacenan o tienen acceso a la información confidencial de Harvard son capaces de proteger adecuadamente la información y deben exigir que dichos terceros protejan la información.

15. Cualquier pérdida real o sospecha de robo, uso indebido o acceso a la información confidencial de Harvard debe ser reportada.

16. Dentro de cada política anteriormente mencionada, Harvard específica cada política y sus actores implicados dentro de esta; además de brindar pautas para cumplirla o, requerimientos.

Ej:

Política 2.

Todos los usuarios son responsables de proteger sus contraseñas de Harvard y otras credenciales de acceso contra el uso no autorizado.

Usuarios

Contraseñas comprometidas: Las contraseñas deben ser cambiadas cuando haya sospecha de que han sido comprometidas.

Contraseñas diferentes: Deben usarse contraseñas diferentes tanto para cuentas pertenecientes a Harvard como para las que no.

No compartir contraseñas: Las contraseñas de usuarios y otras credenciales de acceso nunca deben ser compartidas.

Proteger contraseñas: Todas las contraseñas y credenciales de acceso deben ser protegidas.

Fortalecer contraseñas: Las contraseñas utilizadas en todos los sistemas de Harvard deben tener suficiente longitud y complejidad para protegerlas razonablemente de ser adivinadas por seres humanos o computadoras. (La mayoría de los sistemas de Harvard aplican estándares de longitud y complejidad.)

Servidores

Contraseñas complejas: Los servidores y las aplicaciones que administran contraseñas deben forzar la configuración de una contraseña compleja, véase cómo construir contraseñas fuertes en la página de la universidad de Harvard [51].

Detección de malware: Los servidores deben estar ejecutando el software de detección de malware con archivos de firma actualizados.

Contraseñas almacenadas: Los sistemas que manejan las contraseñas de usuarios deben estar diseñados de tal manera que las contraseñas no sean recuperables por los administradores.

6.2.3 McGill University - Montreal, Canadá.

Política del buen uso de los recursos informáticos de McGill

Los recursos de McGill en TI están destinados a brindar soporte a la misión educativa de la Universidad y a promover el auge del conocimiento mediante la enseñanza, la investigación académica y el servicio a la sociedad. La universidad ofrece las condiciones propicias para acceder al conocimiento e intercambio de información. La universidad está encargada de vigilar el funcionamiento eficaz y fiable de nuestros sistemas y de la protección de nuestros recursos en las tecnologías de la información. La presente política precisa las responsabilidades de la Universidad y los miembros de la comunidad universitaria alusivas al buen uso de los recursos de TI de McGill:

Principios

1. Los recursos TI de McGill apoyan la misión de la universidad en materia de enseñanza, investigación y administración.

2. Los usuarios autorizados deben utilizar los recursos de TI de manera ética, responsable y lícita, conforme a las políticas de la Universidad.

3. Los usuarios autorizados están en el derecho de esperar un respecto adecuado de sus vidas privadas dentro del uso de los recursos TI de McGill.

4. Los usuarios autorizados deben tomar todas las medidas razonables para proteger la confidencialidad, integridad y disponibilidad de los recursos de TI de McGill.

5. Los usuarios autorizados no pueden acceder a los recursos TI de McGill que conforman las políticas y procedimientos de la Universidad. La posibilidad de acceder a los recursos de McGill no es necesariamente sinónimo de autorización para hacerlo.

6. Los usuarios autorizados deben respetar la propiedad intelectual y comercial, incluyendo pero no limitando las marcas comerciales y los derechos de autor, el propietario del software y los datos almacenados por los recursos de TI McGill o transmitida por ellos, incluyendo los recursos de las bibliotecas y archivos.

Información personal

1. Los usuarios autorizados no deben compartir su información personal con otras personas. Cuando es necesario que una cuenta sea compartida y la aplicación no hace posible su delegación, el usuario autorizado debe utilizar los datos personales solo para dicho uso específico.

2. Los usuarios autorizados deben identificarse adecuadamente en aplicaciones, servicios o conexiones que hacen uso de McGill recursos de TI. Un usuario autorizado no debe hacerse pasar por otra persona.

3. No obstante lo dispuesto en los puntos 1 y 2, los usuarios autorizados pueden permanecer en el anonimato cuando sea necesario o legítimo, como en el caso de la participación en algunas encuestas o sondeos.

Seguridad

1. Los usuarios autorizados deben tomar todas las medidas necesarias para proteger la seguridad de

los recursos TI de McGill y cumplir con las políticas y procedimientos de la Universidad relativos a la protección de datos y la gestión de documentos.

2. Los usuarios autorizados no deben utilizar los recursos de McGill de TI con el fin de plantear un riesgo para la seguridad de la Universidad.

3. Los usuarios autorizados deben cumplir con los protocolos de la Universidad para informar sobre las amenazas de seguridad y deben cooperar con las investigaciones sobre posibles violaciones.

4. Las personas que utilizan los recursos TI de una manera que constituye una infracción de las políticas y procedimientos de McGill, si van más allá de su autoridad están en riesgo de que sus actividades sean monitoreadas y grabadas por los administradores del sistema. Durante la supervisión del uso indebido de los recursos de TI o durante el mantenimiento o actualización de los recursos, las actividades de los usuarios autorizados pueden ser monitoreadas también.

Entre otro de los apartados a resaltar y muy importantes son:

Sitios Web Públicos

1. Un usuario autorizado que publica información sobre un tema sitio web público McGill debe asegurarse de que el contenido está en conformidad con las políticas y procedimientos de la Universidad.

2. Cuando McGill realice un patrocinio en un sitio web colaborativo (blogs, wikis o redes sociales), el sitio debe cumplir con las directrices de TI.

3. Ninguna publicidad externa o comercial debe aparecer en sitios web públicos de McGill, sin la autorización previa del CSI, quien debe acudir a un miembro de la alta administración. No obstante esta disposición, las actividades de la universidad, incluyendo pero no limitando las conferencias académicas, seminarios y actividades similares, pueden anunciarse en los sitios web de McGill en cuestión.

4. Las unidades administrativas de McGill deben alojar su sitio web en el sistema de edición del sitio web de la universidad a menos que los requisitos funcionales de las unidades académicas no puedan ser soportados por dicho sistema de edición.

Red

1. Los servicios de TI no suelen tener que utilizar tecnologías que impidan a un usuario autorizado de los recursos TI de McGill, tener acceso a un sitio web externo cuando el equipo se ha configurado para tener acceso a internet.

2. No obstante, de lo anteriormente mencionado, la Universidad puede moderar, filtrar, limitar o bloquear el tráfico de internet cuando se expone a la Universidad o a los usuarios autorizados de amenazas de seguridad, o cuando sea necesario para asegurar la confidencialidad, integridad o disponibilidad de recursos de TI de McGill.

Están estipuladas otras normas para el uso adecuado de la red de la universidad.

Administración de Sistemas

1. Todos los recursos de TI de McGill deben tener un administrador de sistema designado. Cuando una unidad académica no ha realizado previsiones para este propósito, los investigadores o sus delegados son directores de los sistemas de investigación que controlan.

2. Los administradores de sistemas deben cumplir con las políticas establecidas por los procedimientos y protocolos de la universidad y, configurar y gestionar los sistemas de acuerdo con las mejores prácticas de la Universidad y las disposiciones de esta política.

3. Como parte de la ejecución de sus funciones, los administradores de sistemas pueden monitorizar o acceder de manera rutinaria a las cuentas o hacer uso de software y herramientas de hardware (incluyendo herramientas para el seguimiento o control, cookies, registro de auditoría de seguridad y la conexión logs, copias de seguridad y archivos) para supervisar y mantener la actividad del sistema. No deben utilizar estos datos como parte de la autoridad legítima que se asigna a ellos y deben tratar a todos los datos consultados como confidenciales.

A nivel nacional, pocas universidades hacen público sus políticas de seguridad de la información, sin embargo recientemente se ha tratado de agilizar la imposición y capacitación a los miembros de éstas debido al gran aumento de las Tecnologías Informáticas y los riesgos a los que exponen la información en sus entidades día a día; además muy pocas poseen recomendaciones de buenas prácticas de seguridad informática y de la información acordes a sus políticas.

Entre estas instituciones educativas, a continuación se citan las de una universidad:

- Universidad ICESI - Cali, Valle del Cauca.[52]

6.2.4 Política de Seguridad de la Información - Universidad ICESI

A continuación se mencionan los lineamientos generales:

1. La información debe ser protegida: La información es un activo vital de la Universidad y por lo tanto debe ser protegida por todos.

2. La información debe contar con un responsable: Toda la información utilizada por la Universidad para el desarrollo de sus actividades debe tener asignado uno o más responsables, quienes tomarán las decisiones que sean requeridas para su protección y determinarán los privilegios de uso. Así mismo, todas las personas que integran la comunidad universitaria son responsables de la seguridad de la información que reciben por parte de la institución. De igual manera, la seguridad de la información personal es responsabilidad de cada integrante de la comunidad universitaria.

3. La información debe ser clasificada: Los responsables de la información deben clasificarla basados en su valor, sensibilidad, riesgo de pérdida y/o requerimientos legales de retención.

4. El manejo de la información debe cumplir con las regulaciones legales: La comunidad universitaria se compromete a cumplir con la regulación nacional e internacional de seguridad de la información.

5. La propiedad intelectual de la información se debe preservar: Mientras se tenga una relación contractual o como estudiante, la propiedad intelectual sobre investigaciones realizadas, libros o revistas escritas, patentes o derechos de autor, será propiedad de la Universidad, de acuerdo al reglamento de propiedad intelectual de la Universidad Icesi.

6. La seguridad de Información deberá ser parte de la gestión de los sistemas de información de la Universidad: Los requerimientos de seguridad de la información deben ser identificados, antes del diseño de los nuevos sistemas de información, durante los ajustes de los sistemas actuales y durante los cambios tecnológicos que se requieran. De tal manera que se asegure el cumplimiento de la política de seguridad de la información.

7. Se debe asegurar la autenticidad de la información generada por la Universidad: Se deberá asegurar la autenticidad de las comunicaciones electrónicas internas y externas que realice la Universidad.

8. La seguridad de la información será de conocimiento imperativo para la comunidad universitaria: Es obligación de la comunidad universitaria, sin excepción alguna, conocer, respetar y cumplir las políticas de seguridad de la información de la Universidad, desde su ingreso hasta su retiro.

9. Debe existir capacitación continua y creación de cultura en seguridad de la información: La Universidad dispondrá de un programa permanente de creación y consolidación de la cultura de la seguridad de la información. En estos programas deben participar los colaboradores, profesores, estudiantes y terceros.

10. La comunidad universitaria debe comprometerse a usar adecuadamente los servicios y recursos de información: Los servicios y recursos de información de la Universidad son únicamente para propósitos de la institución y deben ser usados como activos para la realización del trabajo requerido.

11. La identificación y autenticación a cualquier activo será personal: El acceso a cualquier información o activo de información de la Universidad debe estar controlado mediante una autenticación personal.

12. Debe existir un control y una administración del acceso a la Información: Se deben establecer mecanismos de control de acceso físico y lógico para prevenir accesos no autorizados a los activos que almacenan la información de la Universidad. La información confidencial de la institución debe mantenerse con acceso restringido cuando no es utilizada. La comunidad universitaria debe respetar esos controles.

13. Debe existir un plan de administración de incidentes: Se contará con un programa de manejo de incidentes que permita gestionar y resolver las situaciones o acciones que violen la política de seguridad.

14. Debe existir una gestión del riesgo en seguridad de la información: Los riesgos a que está expuesta la información y los activos de información de la Universidad, deben ser identificados, evaluados y mitigados de acuerdo a su valor, probabilidad de ocurrencia e impacto.

15. Debe existir un plan de continuidad del negocio para la Universidad: Todos los activos de información y los procesos asociados a los objetivos institucionales deben contar con un plan de continuidad, un plan de recuperación de desastres, y estar preparados para ataques contra la seguridad de la información.

16. Deben existir mecanismos de seguridad para los servicios de red de la Universidad: Se debe asegurar la confidencialidad, integridad y disponibilidad de la información trasmitida sobre la red institucional de la Universidad.

17. Los terceros que utilizan y/o accedan, local y remotamente a los activos de información de la Universidad están obligados a cumplir con la política de seguridad de la información: El uso o acceso por parte de terceros a los activos de información de la Universidad que sean clasificados como confidenciales, debe ser formalizado por medio de acuerdos que hagan obligatorio el cumplimiento de la política de seguridad de la información.

En los sistemas de información de la Universidad del Valle se encuentran unas políticas de seguridad informática, establecidas en el 2008 a través de una consultoría realizada en la oficina de informática OITEL. La cual tiene estipulado ciertas recomendaciones en el manejo de los recursos informáticos en la universidad[1], empero no le permite tener claro la importancia en formación de seguridad informática a muchos de sus miembros (véase Resultados de encuesta Capítulo 7.2) para los procedimientos a la hora de tratar con las tecnologías de información y comunicación que ésta posee; no obstante, en relación a los riesgos o fallas de seguridad, a los que puedan ser expuestos estos sistemas si no hay una divulgación apropiada.

6.3 Marco teórico

6.3.1 Seguridad Informática y de la Información

Aunque estos dos términos están correlacionados y trabajan de manera conjunta, pueden llegar a ser confundidos por lo mismo, sin embargo, tienen funciones diferentes en sus procesos.

La seguridad informática representa ese pilar clave que provee los mecanismos y controles necesarios para resguardar y proteger de manera eficaz los activos informáticos a nivel de Hardware y Software, teniendo así un enfoque en la infraestructura computacional y todo lo relacionado con ésta.

Por otro lado, la seguridad de la información es la disciplina que se encarga de determinar los riesgos, amenazas, análisis de escenarios, las buenas prácticas y esquemas normativos que nos exigen niveles de aseguramiento de procesos en los sistemas de información.

Éste último concepto abarca en cierta manera a la ciberseguridad o seguridad informática, como podemos ver en la Fig. 6.3.1, cualquier pormenor que ocurra en el ciberespacio envuelve información o sistemas de información [53].

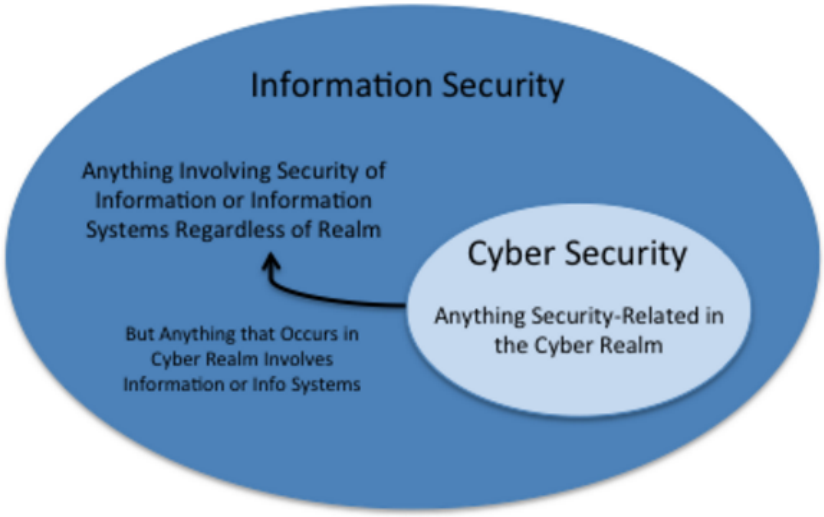

Figure 6.3.1: Seguridad de la Información y Ciberseguridad (o seguridad informática).(Imagen tomada de [5])

6.3.2 Sistema de Gestión de la Seguridad de la Información, SGSI

Según la normativa del estándar ISO 27000 define un SGSI de la siguiente manera:

> "En base al conocimiento del ciclo de vida de cada información relevante , presentado en la Fig. 6.3.2, se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI"[6].

Figure 6.3.2: Ciclo de vida de la Información. (Imagen tomada de [6])

6.3.3 Servicios de seguridad

Los pilares de la seguridad informática y de la información deben garantizar[53]:

Confidencialidad: Cuando se habla de la confidencialidad de la información, se refiere a la protección de la información de su divulgación a terceros no autorizados.

Integridad: La información es precisa y fiable y no ha sido sutilmente modificada o manipulada por un tercero no autorizado. Ésta incluye:

- Autenticidad: La capacidad de verificar que el contenido no ha cambiado de forma no autorizada.
- No repudio: El no repudio en una comunicación le sirve a los emisores o a los receptores para negar un mensaje transmitido. Cuando un mensaje es enviado, el receptor puede probar que el mensaje viene dirigido por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje lo recibió el presunto receptor.

Disponibilidad: La información y otros activos críticos son accesibles para los clientes y el negocio cuando sea necesario. Se debe tener en cuenta, que la información no está disponible no sólo cuando se pierde o se destruye, sino también cuando el acceso a la información es negada o retrasada (es decir, la información está disponible en un sitio web, pero el servidor se siente abrumado por un ataque de denegación de servicio y nadie puede acceder a ella).

6.3.4 Mecanismos de seguridad informática

Los distintos tipos de mecanismos que se pueden utilizar [54–56], se clasifican de acuerdo al objetivo principal del mismo en:

Preventivos: la finalidad de este medio es eludir cualquier tipo de ataque en los sistemas informáticos. Los utilizan en el monitoreo de la información y de los bienes, en los registros de actividades que realiza la organización, en el control de los activos y de los sujetos que acceden a estos.

Detectores: el objetivo de estos es descubrir cualquier tipo de anomalía que sea amenaza para los bienes. Un ejemplo son las personas o equipos de monitoreo encargados de prestar un análisis y estar al margen de encontrar cualquier tipo de intruso dentro de la organización.

Correctivos: estos responden a los incidentes presentados a causa de algún ataque ya realizado dentro de la organización, su finalidad es modificar el estado del sistema para que vuelva a su estado original y adecuado; realizando reparaciones de errores o daños causados.

Disuasivos: su intención es apaciguar a los amenazantes para que no comentan los ataques y así poder minimizar el impacto negativo que puedan tener los bienes.

La mayoría de las TI están conectadas dentro de las organizaciones, entre los importantes mecanismos que deben llevarse a cabo para proporcionar seguridad a la comunicación de todos los partícipes están:

Seguridad física: permite la limitación del acceso a los recursos claves de la red, manteniéndolos detrás de una puerta cerrada y protegida a los desastres naturales y humanos a medida. Brindará protección a los malos usos involuntarios de los equipos de la red por los empleados no capacitados y contratistas; de la misma manera que puede impedir ataques de piratas informáticos, las cambiantes configuraciones de los equipos y otros tipos de amenazas. Unos ejemplos de éstas pueden ser los eventos terroristas y de riesgo biológico, incluyendo bombas, derrames radioactivos, etc.

Autenticación: la mayoría de las políticas de seguridad afirman que para acceder a una red y sus servicios, el usuario debe introducir un nombre de usuario y contraseña que sea autenticado por un servidor de seguridad. La autenticación se basa tradicionalmente en una de las tres siguientes pruebas:

- Algo que el usuario sabe: generalmente implica el conocimiento de un secreto único que es compartido por las partes de autenticación. Para un usuario, este secreto se presenta como una contraseña clásica, un PIN o una clave criptográfica privada.
- Algo que el usuario tiene: el usuario debe poseer físicamente algún elemento físico y único. Un ejemplo serían las tarjetas de contraseña de tokens, tarjetas de seguridad y llaves de hardware.
- Algo que el usuario es: una verificación física única del usuario es necesaria, tal como una huella digital, patrón de retina, voz o rasgos faciales.

Muchos sistemas utilizan la autenticación basándose en dos factores, es decir que el usuario posee dos pruebas de identidad.

Autorización: mientras que la autenticación se encarga de manejar el acceso a los recursos de la red, la autorización dice lo que pueden hacer después de haber accedido a los recursos; otorgando privilegios a los procesos y usuarios. Se recomienda el uso del principio de privilegios mínimos en la autorización de la aplicación, el cual se basa en la idea de que a cada usuario se le debe conceder el mínimo de permisos necesarios para una tarea determinada.

Contabilidad y Auditoría: para analizar con eficacia la seguridad de una red y para responder a los incidentes de seguridad, deben establecerse procedimientos para la recogida de datos de la actividad de la red. A la recopilación de datos se le denomina contabilidad o auditoría. Los datos presentes en la auditoría deben incluir todos los intentos por lograr la autenticación y autorización de cualquier persona, los nombres de usuarios y host de inicios y cierres de sesión. La auditoría no debe obtener las contraseñas, puesto que esto crea un potencial fallo de seguridad; ni contraseñas correctas o incorrectas. Otra parte fundamental es la evaluación de seguridad a la que se debe someter periódicamente en busca de vulnerabilidades en la red, teniendo como resultado un plan específico para la corrección de deficiencias, que pueden ser tan simples como la readaptación del personal profesional.

Cifrado de datos: es un proceso que codifica los datos para protegerlos de ser leídos por nadie más que el receptor previsto. Un dispositivo de encriptación encripta los datos antes de colocarlo en una red. Un dispositivo de descifrado desencripta los datos antes de pasarlo a una aplicación. Un router,

servidor, sistema final o dispositivo dedicado puede actuar como un dispositivo de cifrado o descifrado. Los datos que se cifran se denomina datos cifrados (o simplemente cifrado de datos). Los datos que no están cifrados se llaman textos planos o textos claros. El cifrado es una característica de seguridad útil para proporcionar confidencialidad de los datos. También se puede utilizar para identificar el remitente de los datos. Aunque autenticación y autorización también deben proteger la confidencialidad de los datos e identificar los remitentes, el cifrado es una buena característica de seguridad a aplicar en el caso de que los demás tipos de seguridad fallan.

Filtros de paquetes: Los filtros de paquetes se pueden configurar en los routers, firewalls y servidores para aceptar o denegar paquetes de direcciones o servicios particulares. Estos filtros aumentan los mecanismos de autenticación y autorización. Ellos ayudan a proteger los recursos de red del uso no autorizado, robo, destrucción y ataques de denegación de servicio. Una política de seguridad debe indicar si los filtros de paquetes deben aplicar una u otra de las siguientes políticas:

- Denegar tipos específicos de paquetes y aceptar todo lo demás.
- Acepte tipos específicos de paquetes y negar todo lo demás.

La primera política requiere un conocimiento profundo de las amenazas de seguridad específicos y puede ser difícil de implementar. La segunda política es más fácil de aplicar y más seguro debido a que el administrador de seguridad no tiene que predecir futuros ataques para los que se les debe negar los paquetes. La segunda política es también más fácil de probar porque hay un conjunto finito de usos aceptados de la red.

Cortafuegos: un firewall es un dispositivo que hace cumplir las políticas de seguridad en la frontera entre dos o más redes. Son especialmente importantes en el límite entre la red de la empresa e internet. También es conocido como servidor de seguridad, y posee un conjunto de reglas que especifica cuál tráfico debe ser permitido o denegado. Éste puede realizar un seguimiento de las sesiones de comunicación y de forma más inteligente permitir o denegar el tráfico. Por ejemplo, un servidor de seguridad de estado, puede recordar que un cliente protegido inició una petición para descargar los datos desde un servidor de Internet y permitir los datos de nuevo para esa conexión.

6.3.5 Consideraciones para abordar la construcción del protocolo

A continuación se presentan los conceptos más importantes en el planteamiento del proyecto, que así permitan cimentar una buena base para la elaboración del protocolo; permitiendo tener claridad y entendimiento de los términos a usar en éste.

6.3.5.1 Protocolos

Un protocolo es un reglamento o una serie de instrucciones que se fijan por tradición o por convenio. Partiendo de este significado, es posible emplear la noción en diferentes contextos. Un protocolo puede

ser un documento o una normativa que establece cómo se debe actuar en ciertos procedimientos. De este modo, recopila conductas, acciones y técnicas que se consideran adecuadas ante ciertas situaciones.

Los protocolos y estándares dentro de una organización son de gran importancia, puesto que estos son las pautas de funcionamiento de la producción, comunicación u operación en un entorno de negocios. En un mundo donde la capacidad de interactuar de forma rápida y eficiente se considera la piedra angular de cualquier negocio, estas directrices pueden proporcionar grandes beneficios a la organización.

6.3.5.1.1 Tipos de protocolos

Los protocolos se clasifican básicamente en tres tipos:

Arbitrados: En este tipo de protocolo se cuenta con una tercera parte que se encarga de proporcionar más confianza en la comunicación de los involucrados. Sin embargo, éste puede ser ineficiente al ser vulnerable a ataques contra el árbitro o juez del protocolo.

Adjudicados: Al igual que los arbitrados se vale de una tercera parte, solo que ésta interactúa siempre y cuando sea necesario.

Auto Implementados: Es el mejor, ya que pueden detectar los problemas durante el proceso y abandonar el protocolo, sin utilizar un árbitro. Garantiza que si alguno realiza un engaño, no obstante los demás van a enterarse. No todas las situaciones son apropiadas para este tipo de protocolo, puesto que la mayoría de estos protocolos requieren una gran cantidad de trabajo de parte de todos los participantes.

6.3.5.1.2 Protocolo de Seguridad

Un protocolo de seguridad permite seguir un procedimiento que se ajuste a las leyes, reglas y prácticas que regulan el manejo, protección y distribución de información en función de las potenciales amenazas, es decir, una política de seguridad. Para establecerlo es necesario realizar un análisis de las amenazas y una cuantificación de los riesgos. Deben proporcionarse mecanismos adecuados que aseguren la protección de cada elemento o recurso amenazado.

La información comprometida entre los sistemas informáticos implica la existencia de una arquitectura de comunicaciones común en varios niveles, dentro de los cuales se realizan distintas funcionalidades propias para el intercambio de datos. Se deben hacer uso de mecanismos, servicios y funciones de seguridad que se apoyen, en muchos casos, en servicios, mecanismos y funciones ya implementados en la propia arquitectura de comunicaciones; la estructura de aquellos comportamientos de los procesos de seguridad es lo que denominamos Arquitectura de Seguridad.

Acorde a la política de seguridad, los servicios de seguridad utilizan los mecanismos implementados en la arquitectura de seguridad, los cuales implican en la mayoría de casos un intercambio de unidades de datos entre dos entidades y la realización de determinadas funciones aplicadas a estas unidades (cifrado, cálculo de redundancia, etc). Esta comunicación que tiene como objeto implementar un servicio de seguridad (un auténtico protocolo) es lo que se denomina Protocolo de Seguridad.[57]

En los protocolos de seguridad, la protección y autenticidad del intercambio de información son dos aspectos muy importantes, para los cuales existen determinados protocolos: los de gestión y distribución de claves, y los de autenticación.

6.3.5.1.2.1 Protocolos de gestión y distribución de claves

Los protocolos de distribución de claves se clasifican dependiendo del sistema criptográfico(cifrado) usado. La criptografía se ocupa de enviar información en un medio inseguro, encriptandola, para que no pueda ser vista o manipulada por un tercero no autorizado. Existen dos ramas: la criptografía de clave privada o simétrica y la de clave pública o asimétrica.

Criptografía simétrica

La criptografía simétrica o de clave única, permite que los dos entes en comunicación se pongan de acuerdo con una clave secreta compartida entre ellos. Se tiene la información que va a ser transmitida en un medio de comunicación entre las partes y la clave, mediante unas funciones aplicadas sobre la información se realiza una encriptación; el receptor, al conocer la clave compartida con su emisor puede realizar la debida desencriptación de la información cifrada recibida[58].

Paso a paso:

1. Se genera la clave. **2.** Se cifra el mensaje usando la clave. **3.** Se descifra el mensaje usando la misma clave.

Uno de los sistemas criptográficos más conocidos es el DES(Data Encryption Standard). Es un algoritmo de cifrado desarrollado por la NSA a petición del gobierno de EEUU bajo la presión de las empresas por la necesidad de un método para proteger sus comunicaciones. Funciona con un cifrado por bloques. Se toma un bloque de una longitud fija de bits y lo transforma mediante una serie de operaciones básicas en otro bloque cifrado de la misma longitud. En DES el tamaño del bloque es de 64 bits pero 8 de estos se utilizan para comprobar la paridad, dejando como longitud efectiva de la clave 56 bits.

Criptografía asimétrica

La criptografía pública posee dos claves para la transmisión. Una clave pública que es conocida por todo el público, y que es utilizada para el cifrado de la información, y una clave privada que es solamente conocida por el usuario de esa clave y que se utiliza para el descifrado.

Paso a paso:

1. Se genera la clave pública y la clave privada. **2.** Se cifra el mensaje usando la clave pública. **3.** Se descifra el mensaje usando la clave privada.

Un algoritmo de encriptación asimétrica muy conocido es el RSA(Rivest, Shamir y Adleman), desarrollado en el año 1977 por los anteriormente citados. Su procedimiento consta de escoger dos números primos grandes elegidos de forma aleatoria y mantenidos en secreto. La dificultad de este algoritmo, recae en la complejidad para factorizar números grandes.

6.3.5.1.2.2 Protocolos de Autenticación

Los protocolos de autenticación deben garantizar que el origen de la información sea el alegado y no haya sufrido alteraciones. Además, se debe reconocer que ha sido enviado por el debido participante en la comunicación.

Usa funciones que generen un valor añadido a la unidad de datos transferida para que se pueda verificar la autenticidad de los datos y del emisor. Como ejemplos de dichas funciones están las funciones de cifrado/descifrado, código de autenticación o funciones "hash".

La función Hash acepta un mensaje de longitud variable M como entrada, y produce un bloque de tamaño fijo Hash(M), el cual también es llamado resumen del mensaje. Teniendo dicha salida se envía con el mensaje para que el receptor pueda autenticarlo mediante el resumen.

6.3.6 Estándares para la Gestión de la Seguridad de la Información

6.3.6.1 Estándares ISO

La Organización Internacional de Normalización, establecida en 1947, es un organismo internacional no gubernamental que colabora con la Comisión Electrotécnica Internacional (IEC, International Electrotechnical Commission) y la Unión Internacional de Telecomunicaciones (ITU, International Telecommunication Union) en estándares de TIC.

ISO / IEC JTC 1 / SC 27 mantiene un comité de expertos dedicado a la elaboración de normas internacionales de sistemas de gestión de seguridad de la información, también conocido como la familia de normas de un sistema de gestión de la seguridad de la información (SGSI). La Fig. 6.3.3 muestra la relación de la familia de estándares SGSI.

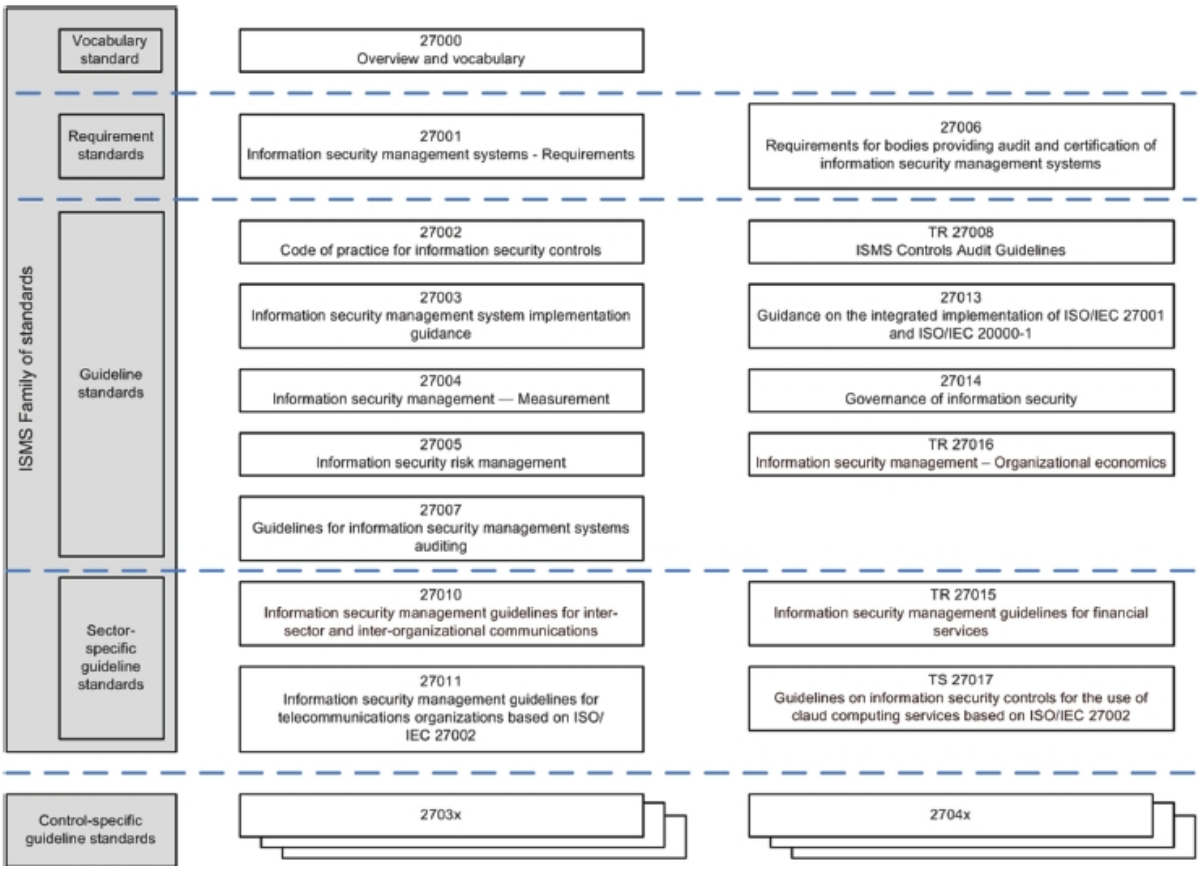

Figure 6.3.3: Relación de la familia de estándares SGSI. (Imagen tomada de [7])

6.3.6.2 ISO-IEC 27001

La norma ISO 27001 permite suministrar múltiples requisitos que permiten el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica de una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.[7]

A continuación se presentan las cláusulas importantes en la norma:

6.3.6.2.1 Contexto de la organización

En este apartado de la norma se tiene como objetivo determinar las cuestiones externas e internas que le competen al logro de la implantación del sistema de gestión de la seguridad de la información. Al identificar las partes pertinentes y tener claro los requerimientos de éstas con respecto a la seguridad de la información, se establece el alcance que tendrá el SGSI para su posterior implementación,

mantenimiento y mejora de acuerdo a los requisitos de la norma.

6.3.6.2.2 Liderazgo

Los entes responsables de la dirección del sistema de gestión de la seguridad de la información deberán demostrar liderazgo y compromiso para establecer una política de seguridad de la información y asegurarse del cumplimiento de los objetivos de la seguridad de la información; que a su vez estos sean compatibles con la organización.

Al implantar una política de seguridad de la información, esta debe cumplir con ser adecuada al propósito de la organización, incluir los objetivos de la seguridad de la información, incluir el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información y el compromiso de mejora continua. No obstante, la política debe estar disponible como información documentada, comunicarse dentro de la organización y estar disponible para las partes interesadas según sea apropiado.

Así pues la alta dirección debe rendir cuentas del desempeño del sistema de gestión de la seguridad de la información.

6.3.6.2.3 Planificación

Se debe realizar una planificación basada en los requerimientos ya mencionados para implantar el SGSI, con el fin de prevenir o reducir efectos indeseados y lograr la mejora continua. Aquí se incluye las acciones de la organización referentes al trato de los riesgos de la seguridad de la información, empezando desde la identificación y análisis de los riesgos de la información, hasta la selección de las opciones apropiadas de tratamiento y control de riesgos, junto con la aprobación del tratamiento de riesgos por parte de los dueños de los riesgos; y realizar la debida documentación.

Por cada objetivo de seguridad de la información deberá haber un plan para lograrlos. Por lo tanto los objetivos deben ser coherentes con la política de seguridad de la información, ser medibles, tener en cuenta los requisitos de la seguridad de la información aplicables, los resultados de la valoración y tratamiento de riesgos, ser comunicados, y ser actualizados en algunos casos. Mediante esta planeación de objetivos la organización deberá saber lo que se va hacer, los recursos que serán requeridos, los responsables, cuando se finalizará cómo se evaluarán los resultados.

6.3.6.2.4 Soporte

Los recursos necesarios para establecer, implantar, mantener y mejorar el SGSI deben ser determinados y proporcionados.

La organización debe determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información. Tomando como medidas la educación, formación o experiencias adecuadas. Cada persona de esas deberá tener conocimiento y conciencia de la política de seguridad de la información y las implicaciones de la no conformidad de los

requisitos del sistema de gestión de la seguridad de la información.

La realización de comunicaciones internas y externas pertinentes al SGSI deben incluir el contenido de la comunicación, el cuándo comunicar, a quién comunicar, quién debe comunicar y los procesos para llevar a cabo la comunicación. El SGSI debe poseer la información documentada requerida por la norma y la necesaria para la eficacia del sistema. Cuando se cree o actualice información debe haber consistencia con el contenido, formato, y la revisión y aprobación con respecto a la idoneidad y adecuación.

6.3.6.2.5 Operación

Se debe tener una planificación, implementación y un control operacional de los procesos necesarios para cumplir los requisitos de seguridad de la información como los procesos contratados externamente.

6.3.6.2.6 Evaluación de desempeño

Es necesario hacer seguimiento y medir el desempeño de la seguridad de la información y la eficacia del SGSI. Teniendo en cuenta los procesos y controles de la seguridad de la información, el cuándo se deben llevar a cabo el seguimiento y la medición, el cuándo se debe analizar y evaluar los resultados del seguimiento y de la medición, y el quién debe evaluar estos resultados.

En este apartado es donde es importante recalcar la realización de auditorías internas a intervalos planificados en la organización, con el objetivo de proporcionar información respecto a si el SGSI es conforme con los requisitos de la organización y los de la norma, además, si está implementado y mantenido eficazmente. Así, la organización planifica, establece, implementa y mantiene uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes.

La alta dirección debe revisar el SGSI a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia continuas.

6.3.6.2.7 Mejora

En este ámbito la norma exige que cuando ocurra una no conformidad, la organización debe reaccionar ante la no conformidad según sea aplicable tomar acciones para controlarla y corregirla y, hacer frente a las consecuencias. Ocurrida ésta, se debe evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante: la revisión de la no conformidad y la determinación de las causas de aquella no conformidad y la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir. Luego del proceso de evaluación de la no conformidad, la organización debe implementar cualquier acción necesaria, revisar la eficacia de las acciones correctivas tomadas, y hacer cambios al SGSI, si es necesario. Todo esto igualmente debe constar en información documentada del SGSI.

6.3.6.3 ISO-IEC 27005 Gestión de Riesgo

La gestión de riesgo es una parte esencial que toda organización debe implementar para poder incrementar la dificultad de que se perpetúen fraudes informáticos que afecten la seguridad de la información. Para esto es de evidente necesidad seguir unas directrices o estándares ya propuestos que permitan efectuar un correcto enfoque en la gestión de riesgo como lo ofrece la norma ISO/IEC 27005 [59], la cual consta de:

6.3.6.3.1 Establecimiento del contexto

En este apartado es pertinente resaltar que toda la información acerca de la organización es primordial para establecer el contexto de la gestión de riesgo en la seguridad de la información. Esto implica establecer criterios básicos necesarios para la gestión apropiada; tales como criterios de evaluación del riesgo, criterios de impacto y de aceptación del riesgo. Agregado a esto, se deben definir el alcance y los límites de la gestión de riesgo de la seguridad de la información, es decir, que todos los activos relevantes son tomados en consideración de la valoración de riesgo; para finalmente establecer una organización adecuada que opere la gestión de riesgo en la seguridad de la información.

6.3.6.3.2 Valoración del riesgo

Aquí se determina el valor de los activos de información, se identifican las amenazas y vulnerabilidades aplicables que existen (o que podrían existir), se identifica los controles existentes y sus efectos en el riesgo identificado; determinando así las consecuencias potenciales y priorizando los riesgos derivados para clasificarlos frente a los criterios de evaluación del riesgo sumidos en el contexto establecido, o dicho de otra manera, brindar la lista de los riesgos valorados y priorizados acorde a los criterios de evaluación del riesgo.

6.3.6.3.3 Tratamiento del riesgo

El objetivo es seleccionar controles para reducir, retener, evitar o transferir los riesgos y definir un plan para el tratamiento del riesgo. Para lo cual la norma propone cuatro opciones:

Reducción del riesgo: se debe reducir el nivel del riesgo mediante la selección de controles; de manera que el riesgo residual pueda evaluarse como aceptable.

Retención del riesgo: no tomar acción posterior dependiendo de la evaluación del riesgo, es decir si el nivel de riesgo satisface los criterios para su aceptación no es necesario implementar controles adicionales.

Evitación del riesgo: debe evitarse la actividad o acción que da origen al riesgo particular.

Transferencia del riesgo: se transferiría el riesgo a otra parte que pueda gestionar de manera más eficaz el riesgo particular.

6.3.6.3.4 Aceptación del riesgo

Aceptar los riesgos y las responsabilidades adyacentes a dicha decisión y registrarla de manera formal como lo sugiere la norma ISO/IEC 27001.

6.3.6.3.5 Comunicación del riesgo

La información acerca del riesgo se debería intercambiar y/o compartir entre la persona que toma la decisión y las otras partes involucradas.

6.3.6.3.6 Monitoreo y revisión del riesgo

Los riesgos y sus factores (es decir, el valor de los activos, los impactos, las amenazas, las vulnerabilidades, la probabilidad de ocurrencia) se deberían monitorear y revisar con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana, y para mantener una visión general de la perspectiva completa del riesgo.

A continuación se ilustra el proceso de Gestión de Riesgos en la Fig. 6.3.4

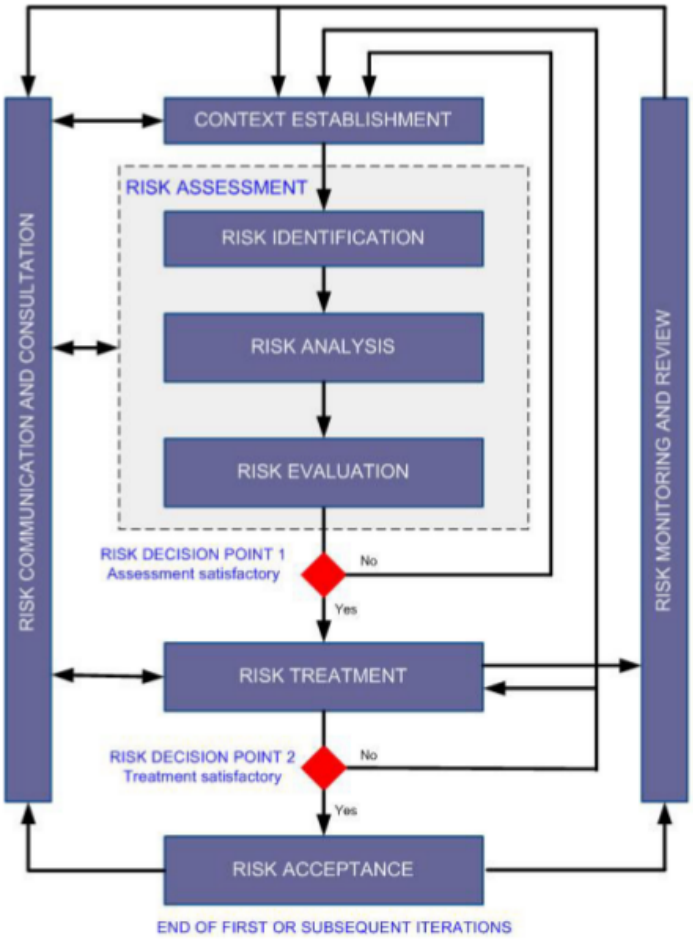

Figure 6.3.4: Proceso de Gestión del Riesgo en la Seguridad de la Información. (Imagen tomada de [7])

6.3.6.4 Activos Informáticos

La gestión de activos de información es cada vez más importante a medida que las organizaciones experimentan una mayor competencia de sus entornos internos y externos. Según la literatura Los activos de información pueden utilizarse para mejorar la eficacia de la organización, y debe tenerse en cuenta para lograr una buena gestión de la seguridad de la información [60]. Si se establecen políticas de seguridad u otros tipos de mecanismos para tratar de manera segura con los activos, es debidamente necesario que estos sean siempre identificados y comprendidos [61].

Los activos informáticos se definen como algo de valor para la organización. Esto incluye los activos intangibles tales como la reputación de la empresa y la información digital y, tangibles como la infraestructura física. Mientras se procede a la identificación de activos, también identifique o confirme el propietario del activo. A menudo es más difícil identificar a la persona o grupo responsable de un activo de lo que puede parecer. Debe documentarse a los propietarios de activos específicos durante las discusiones de riesgo facilitadas. Esta información puede ser útil durante el proceso de priorización con el fin de confirmar la información y comunicar los riesgos directamente a los propietarios de activos. Según sea apropiado para su organización, una tercera definición de activos "servicios TI" puede ser útil. El servicio de TI es una combinación de activos tangibles e intangibles. Por ejemplo, un servicio corporativo de correo electrónico de TI contiene servidores físicos y utiliza la red física; sin embargo, el servicio puede contener datos digitales sensibles. Debe incluirse como un activo porque generalmente tiene diferentes propietarios de datos y activos físicos. Por ejemplo, el propietario del servicio de correo electrónico es responsable de la disponibilidad de acceso y envío de correo electrónico. Sin embargo, el servicio de correo electrónico puede no ser responsable de la confidencialidad de los datos financieros dentro del correo electrónico o de los controles físicos que rodean a los servidores de correo electrónico [8].

En la Tabla 6.3.1 se presentan ejemplos de activos de información extraídos de la Guía de Administración de Riesgos de Seguridad de Microsoft[8], los cuales pueden ser utilizados como referencia para llevar a cabo el inventario de activos si se propone instaurar un sistema de gestión de seguridad de la información en algún proceso de la universidad como trabajo de grado. En el campo de estudio de este trabajo se pretende usar para la identificación de algunos activos que carezcan de una seguridad adecuada en la universidad.

Clasificación de activo	Entorno General TI	Activo
Tangible	Infraestructura Física	Centro de datos
		Servidores
		Computadores de escritorio
		Computadores móviles
		PDA (Computadora de bolsillo)
		Celulares
		Software del servidor de aplicación
		Routers
		Conmutadores de Red (Switches)
		Firewalls
		Medios extraíbles (USB, CD-ROM, Disco duro...)
		Sistemas contra incendios
		Equipos de climatización
		Sistemas de alimentación ininterrumpida (UPS)
	Datos internos	Código Fuente
		Datos de Recursos Humanos
		Datos Financieros
		Datos de Marketing
		Contraseñas de empleados
		Propiedad Intelectual
		Sitios Web Internos
		Diseño de infraestructura de Red
	Datos externos	Datos de contratación de asociados
		Datos financieros de asociados
		Aplicación de sitios web de ventas
		Datos de sitio web de Marketing
Servicios TI	Mensajería	Programación de correo electrónico (como Microsoft Exchange)
		Mensajería instantánea
	Infraestructura básica	Sistema de nombre de dominios *DNS*
		Servidor *DHCP*
		Servicio telefónico
		Acceso a red privada virtual *VPN*
		Servicios inalámbricos *WiFi*
Aplicaciones		Browser
		Cliente de correo electrónico
		Sistema de gestión de base de datos
		Antivirus
		Sistema operativo
		Software licenciado
		Sistema de backup

Table 6.3.1: Activos de Información (Tomada de [8]).

6.3.7 Vulnerabilidades

Una vulnerabilidad es una debilidad de un activo o grupo de activos que una amenaza puede explotar. En términos simplificados, las vulnerabilidades proporcionan el mecanismo o la forma en que pueden ocurrir las amenazas. NIST define la vulnerabilidad como una condición o debilidad en (o ausencia) de procedimientos de seguridad, controles técnicos, controles físicos u otros controles que podrían ser explotados por una amenaza [62]. Como ejemplo, una vulnerabilidad común para los hosts es la ausencia de actualizaciones de seguridad. La incorporación de los ejemplos de amenazas y vulnerabilidad dados anteriormente producen la siguiente declaración: "Los hosts sin parches pueden conducir a un incumplimiento de la integridad de la información que reside en ellos"[8]. Por lo tanto, la relación entre vulnerabilidad y amenaza define un riesgo para la organización[63]. En la Tabla 6.3.2, se exponen ejemplos de vulnerabilidades en diversas áreas de seguridad, e incluye ejemplos de amenazas que pueden explotar estas vulnerabilidades; para consideración del trabajo se tienen en cuenta a la hora de hacer el esbozo de las vulnerabilidades.

Tipos	**Ejemplos de vulnerabilidades**	**Ejemplos de amenazas**
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o de medios
	susceptibilidad a las variaciones de voltaje	Perdida del suministro de energía
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios y documentos
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Ausencia de mecanismos de identificación de usuario	Falsificación de derechos
Software	Tablas de contraseña sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Descarga y uso no controlados de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
Red	Ausencia de pruebas de envió en recepción de mensajes	Negación de acciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Entrenamiento insuficiente en seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Organización	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto e equipos

Table 6.3.2: Ejemplos de vulnerabilidades (Tomada de [8]).

7 Metodología

7.1 Actividades a realizar

7.1.1 Procedimiento

Para llevar a cabo el cumplimiento de los objetivos en los que se propone indagar acerca de la seguridad informática y de la información, sobre protocolos y sobre las normas ISO, se procede a revisar la literatura y terminología de la temática, y se acude a la orientación de la oficina de informática, OITEl, que está a cargo de los procesos de seguridad de la información dentro de la universidad. La OITEL facilita para el trabajo de grado, información de una consultoría de seguridad informática realizada en la universidad del valle donde se evidencia el proceso realizado por ésta y más información confidencial referente al área. Finalmente se establecen reuniones semanales para el acompañamiento. Este proceso se vio continuamente interrumpido por la disponibilidad de la OITEL durante los dos semestres. Sin embargo, se optó por acudir a miembros de la Universidad Autónoma de Occidente expertos en el área para recibir recomendaciones y una mejor dirección en el cumplimiento de los objetivos y en el desarrollo del trabajo de grado.

El objetivo 3 del trabajo de grado, que dictamina realizar la clasificación de información que hacen uso de tecnologías informáticas, y las respectivas funcionalidades realizadas por la comunidad universitaria con éstas, fue propuesto cumplirlo mediante dos encuestas y una entrevista, sin embargo el proceso para hacerlas tomó más del tiempo esperado, por la disponibilidad de la OITEL; ya que en primer lugar por la confidencialidad trabajada en el trabajo de grado debían revisar las encuestas y sugerir correcciones

acordes para su divulgación. A continuación se presenta la versión resultante de la encuesta aplicada a los encargados de los sistemas de información:

7.1.1.1 Encuesta a encargados de los sistemas de información

Las siguientes preguntas hacen parte de una investigación tipo cualitativa, para el estudio de los sistemas de información pertenecientes a la facultad de Salud y de Ingeniería en la Universidad del Valle, como objeto de estudio en el trabajo de grado.

1. ¿Qué tipo de información o activos maneja este Sistema de Información (S.I)?

2. ¿El S.I ha sido víctima de amenazas que comprometen la información?

3. ¿Hay suficiente integridad en los activos que maneja el sistema?

4. ¿Qué riesgos puede correr la organización con la pérdida de esta información que maneja el sistema?

5. ¿Hay un buen control en la jerarquía de confidencialidad de la información? (Autenticación)

6. ¿Cómo protegen la información del sistema?

7.1.1.2 Encuesta a las facultades de la comunidad universitaria

Se realizará una encuesta a los miembros de las facultades de la comunidad universitaria (Profesores, estudiantes, empleados, etc) para complementar el cumplimiento del objetivo de clasificar la información de la que hacen uso los usuarios de la universidad y aplicaciones (como sistemas operativos, *firewalls* o antivirus); además de dar una visión general de cultura de riesgo de la seguridad informática y de la información desde la perspectiva de los miembros de la institución.

Las preguntas de la encuesta estarán en conjunto con los resultados.

7.1.1.3 Entrevista OITEL (Oficina de Informática Y Telecomunicaciones)

Se llevó a cabo una entrevista con el director encargado de la oficina de informática y telecomunicaciones de la OITEL para dar respuesta a ¿cuál es la cultura de riesgo de la universidad? desde su perspectiva como responsable de la protección de los datos de los sistemas de información de la universidad.

Preguntas:

1. Defina la importancia de la seguridad informática y de la información en la universidad.

2. ¿Qué políticas de seguridad informática y de la información maneja la universidad?

3. ¿De qué manera se brindan capacitaciones en el ámbito de la seguridad informática y de la información?

4. ¿Bajo qué normatividad la universidad orienta el desarrollo de éstas políticas?

5. ¿Qué problemas u obstáculos presenta la universidad en cuanto a la gestión de la seguridad de la información?

6. ¿Se han presentado delitos informáticos en la universidad? y ¿Cuales han sido las causas?

7.1.2 Recopilación de datos

Para la recolección de datos se decidió firmar un acta de confidencialidad con la OITEL junto con mi director de tesis, la cual está adjunta como anexo, y era necesaria para avanzar con la investigación. A continuación se especifican los mecanismos para la recolección de datos en cada actividad realizada:

1. Los datos para la encuesta a los miembros de la facultad de salud y de ingeniería fueron tomados vía correo electrónico, adjunto el acta de confidencialidad.

2. Para la encuesta a los usuarios de la universidad, se divulgó la encuesta vía correo electrónico, a través de una aplicación web de Google Drive, conocida como Google Forms. La cual permitió la creación del formulario y posteriormente para los participantes facilitaba el acceso solo a través del correo universitario y fue enviado a un conjunto de la comunidad universitaria. Se capturó adecuadamente la información durante dos días y fue debidamente cerrado el formulario; la OITEL participó como mediadora para la dispersión del sondeo.

3. Para la entrevista en la OITEL se usó una grabadora.

7.1.3 Análisis de datos

Posterior a la toma de datos se tuvo en cuenta:

1. Para el análisis de la encuesta a los administradores de sistemas de información se acudió a una reunión con los participantes para revisar las conclusiones de la encuesta y la finalidad por la que fue propuesta, además de su opinión respecto a la temática.

2. En el caso de la encuesta a la comunidad universitaria, se hizo acopio y análisis de los datos a través de la misma aplicación que se tomó como herramienta para la recopilación de datos, Google Forms; la cual permitió extraer a Microsoft Excel los datos para ser analizados estadísticamente a través de histogramas y diagramas de pastel.

3. De la entrevista, por haberse llevado a cabo con el director de la oficina de informática, directo responsable de la seguridad de la información en la universidad del valle, se logró inferir varias conclusiones sobre la información proporcionada de los hechos reales sobre la temática en la universidad; que aportaron significativamente al trabajo de grado.

7.1.4 Calidad de datos

El control de la calidad de una investigación cualitativa es un proceso de verificación que no corresponde a una tarea lineal y segmentada, sino, por el contrario, es un proceso reiterativo y constante durante todo el proceso investigativo [64]. Por esto el análisis de datos se realizará de forma concomitante a lo largo de todo el proceso de investigación, ya que la investigación cualitativa no culmina en el proceso de investigación, sino que es un ejercicio permanente que se inicia con el diseño del proyecto y que va guiándose a partir de la información que se recoge.

Para garantizar la **credibilidad** (validez interna) se tuvo en cuenta:

1. Un diseño adecuado de la muestra acorde al objetivo planteado para la encuesta, sin embargo a medida que el proyecto avanzaba se veían posibilidades de complementar un mejor diseño de las encuestas pero por el tiempo de revisión con la OITEL no fue posible agregar esos cambios.

2. Revisión de los resultados con algunos participantes.

3. Triangulación con revisores externos.

Para asegurar la **transferibilidad** (validez externa) se hizo un diseño adecuado que fuese posible extendido a otros contextos, como por ejemplo, llevar el mismo tipo de encuestas o mejoradas a una facultad diferente de la universidad.

Para garantizar la **dependencia** (confiabilidad) se tuvo en cuenta el desarrollo sistemático y descripción del análisis, la cantidad de datos como muestra y un analista externo.

8

Resultados de encuestas y entrevista

8.1 Encuesta a encargados de los Sistemas de Información

La Universidad del Valle tiene múltiples sistemas de información que hacen uso de tecnologías informáticas, en adición al cumplimiento del objetivo sobre **la clasificación de la información y aplicaciones en todas la áreas que hacen uso de TI** y en respuesta a la cultura de seguridad informática de los administradores de estos, se realizó una corta encuesta "Seguridad Informática y de la Información de los Sistemas de Información de las Facultades de Salud e Ingeniería de Sistemas" en las vicedecanaturas de las respectivas facultades.

Como resultado de la encuesta en base a las observaciones realizadas por el analista externo, se destaca que los administradores de los sistemas de información:

1. Desconocían tener alguna guía que proporcionara orientación sobre recomendaciones de buenas prácticas de Seguridad Informática y de la Información para el manejo del sistema de información.

2. Relacionaban el proteger la información solamente hacia agentes externos, sin tener en cuenta los riesgos internos, que evidentemente son altos, puesto que su desconocimiento evidencia que no han sido capacitados para el manejo seguro de la información.

3. Eran conscientes de las consecuencias que podrían tener al sufrir pérdidas de información en los sistemas y que sabían qué acciones tomar respecto a este problema, más no tenían una guía detallada de los riesgos y medidas a tomar.

4. Asociaban la respuesta de incidentes o problemas de la seguridad de información como respons-

abilidad únicamente de la OITEl.

El tipo de información que se maneja en la facultad de Ingeniería es netamente académica y corresponde a las siguientes aplicaciones o sistemas de información:

1. Sistema de Soporte para la Asignación y Registro de las Actividades Académicas de los Profesores de la Facultad de Ingeniería (SSARA): La información manejada compete a la carga académica de los docentes.

2. Gestor de Anteproyectos y Trabajos de Grados de Ingeniería Química (GATGIQ): en los que la información manejada son los anteproyectos y trabajos de grado.

Por parte de la facultad de salud, no fue proporcionada esta información, por inquietudes frente a la confidencialidad de la información y sugirieron no darla. Por último se logró reunirse con los participantes y afirmaron ver la seguridad de la información como algo importante de lo que deben ser capacitados, pero que sin embargo era la OITEL la encargada de hacerse cargo de cualquier problema relacionado con la materia.

8.2 Análisis de la encuesta a la comunidad de la Universidad Del Valle

A continuación se exponen los resultados de participación, teniendo primero la facultad, seguido del número de participantes con el porcentaje de los 414 usuarios:

Ingeniería, 165 (39,7%).
Humanidades, 60 (14,5%).
Ciencias de la Administración, 48 (11,6%).
Salud, 40 (9,7%).
Ciencias Naturales y Exactas, 31 (7,5%).
Institución de educación y pedagogía, 23 (5,6%).
Ciencias Sociales y Económicas 20 (4,8%).
Artes Integradas, 18 (4,4%).
Institución de psicología, 9 (2,2%).

Pregunta, resultado y análisis:

1. ¿Sabe acerca de la importancia de la seguridad Informática y de la información?:

- Sí.
- No.

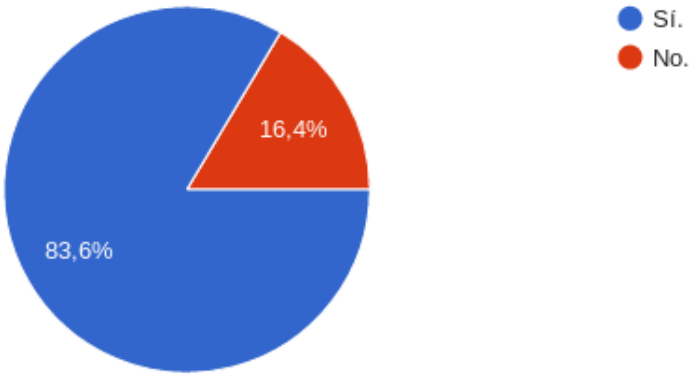

Figure 8.2.1: ¿Sabe acerca de la importancia de la seguridad Informática y de la información?:

Análisis: El 83,6% de los miembros participantes de la encuesta realizada a la comunidad universitaria saben acerca de la importancia de la seguridad informática y de la información. Mientras existe un 16,4% que no. Lo cual nos indica que gran mayoría de la muestra estudiada no ha tenido una formación educativa adecuada en el área de estudio.

2. ¿Conoce la diferencia entre "Seguridad Informática" y "Seguridad de la Información"?

- Sí.
- No.

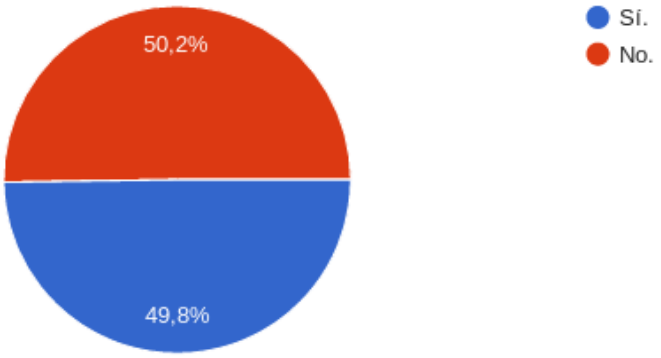

Figure 8.2.2: ¿Conoce la diferencia entre "Seguridad Informática" y "Seguridad de la Información"?

Análisis: Existe una diferencia mínima (0.4%) entre los que dicen conocer la diferencia entre seguridad informática y de la información. 208 encuestados dijeron no conocer la diferencia, mientras los otros 206 restantes, afirmaron conocer la diferencia.

3. La "Seguridad Informática" y la "Seguridad de la Información" son:

- Lo mismo.
- No están relacionadas.
- La ”Seguridad de la Información” abarca la ”Seguridad Informática”.
- La ”Seguridad Informática” abarca la ”Seguridad de la Información”.
- No sabe.

Figure 8.2.3: La "Seguridad Informática" y la "Seguridad de la Información" son

Análisis: En esta pregunta el objetivo era filtrar a quienes afirmaron conocer la diferencia para ver si acertaban. Es decir, se concluyó de los 206 que sabían la diferencia, estaban errados el 74,3%; y solo el 25,7% contesto la respuesta correcta que era ”La seguridad de la información abarca la seguridad informática”.

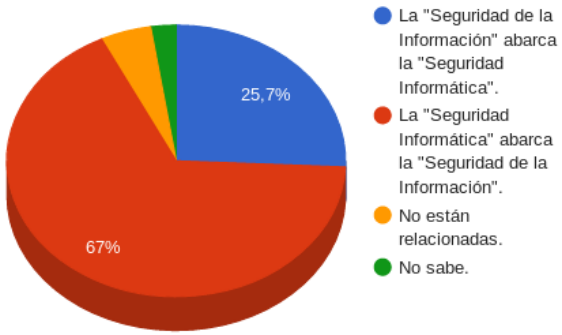

Figure 8.2.4: Filtro diferencia "Seguridad Informática" y la "Seguridad de la Información".

4. Indique la importancia (baja, media, alta o no importante) de la Seguridad Informática y de la Información en:

- Académico

- Personal

Figure 8.2.5: Indique la importancia de la Seguridad Informática y de la Información.

Análisis: La importancia de la seguridad informática y de la información en el contexto académico y en el personal, demostró ser bastante alta; dándole un 14,7% de mayor peso que la académica.

5. ¿Qué tipo de TI (Tecnologías Informáticas) utiliza en la universidad?

- Accesorios propios.
- Equipos de computo de la universidad.
- Accesorios propios y equipos de la universidad.
- Ninguna.

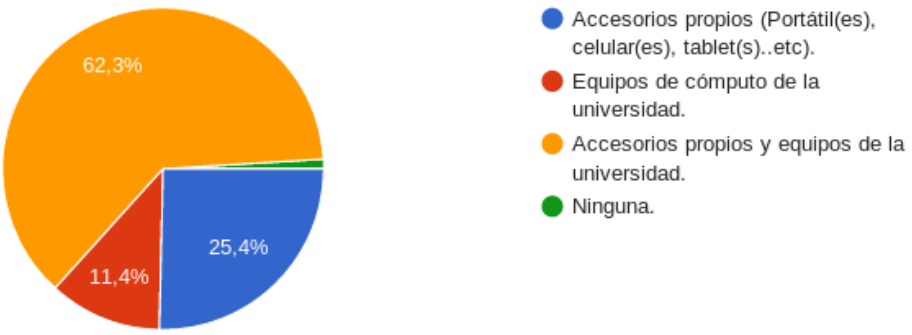

Figure 8.2.6: ¿Qué tipo de TI utiliza en la universidad?

Análisis: Un 73,7% usan los equipos TI de la universidad. Y un 87,7% usa sus equipos propios dentro de la universidad.

6. Si utiliza equipos propios, ¿qué tipo de protección le brinda a sus accesorios tecnológicos?

- Firewall y/o antivirus.
- Contraseñas.
- Todas las anteriores.
- Ninguna.

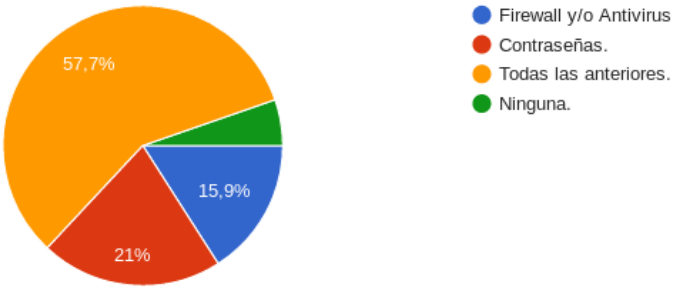

Figure 8.2.7: ¿Qué tipo de protección le brinda a sus accesorios tecnológicos?.

Análisis: 66 participantes utilizan firewall y/o antivirus para proteger sus equipos TI, 87 utilizan únicamente contraseñas, 239 utilizan ambos mecanismos de protección, y unos 22 no utiliza ningún mecanismo de estos.

7. ¿Los equipos de la Universidad tienen todos los medios de protección anteriormente mencionados?

- Sí.
- No.
- No sabe.

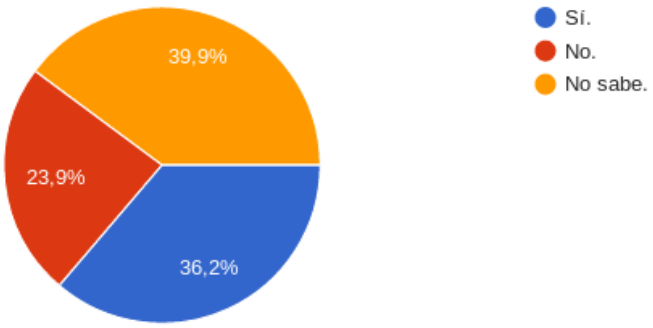

Figure 8.2.8: ¿Los equipos de la Universidad tienen estos medios de protección?

Análisis: Aquí los resultados muestran un porcentaje disperso. Un 39,9% no tiene conocimiento si la universidad utiliza todos estos mecanismos de protección en los equipos TI, 36,2% afirma que la universidad si utiliza aquellos tipos de protección. Y un porcentaje un poco menor de 23,9% afirma que la universidad no los utiliza todos en sus equipos de cómputo.

8. ¿Qué sistema operativo (Windows, Linux, Mac, otro) usa en?:

- Equipos de la universidad.
- Equipos propios.

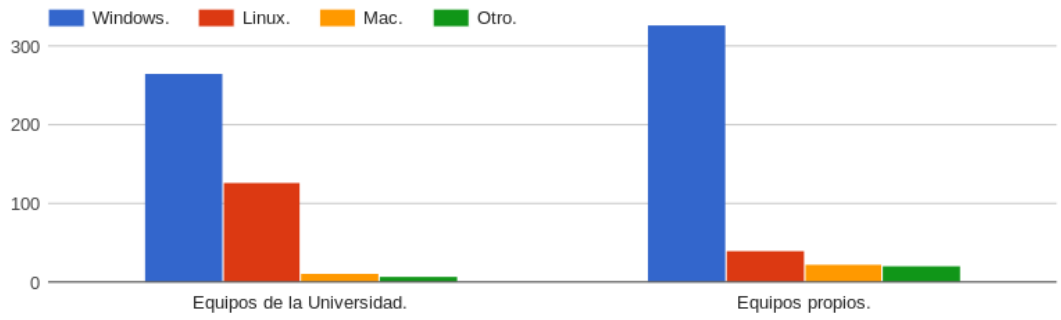

Figure 8.2.9: ¿Qué sistema operativo usa en los equipos de cómputo?

Análisis: Los resultados demuestran que los usuarios usan el sistema operativo Windows como preferencia en la universidad; al igual que en sus equipos propios.

9. ¿Qué clase de información maneja en la Universidad? (Puede seleccionar más de una respuesta):

- Pública de la Universidad. (Información de la Universidad disponible al público; ej: Información de Blogs o páginas web pertenecientes a la Universidad)
- Confidencial o sensible, de la Universidad. (Información comercial o personal de la Universidad para la cual la divulgación no autorizada podría tener un impacto grave en la universidad, individuos o afiliados. Ej: Información de servidores, contraseñas de equipos de cómputo restringidos a otros, etc)
- Académica. (Trabajos, proyectos, etc)
- Personal. (Redes sociales, correos, cuentas bancarias, etc)

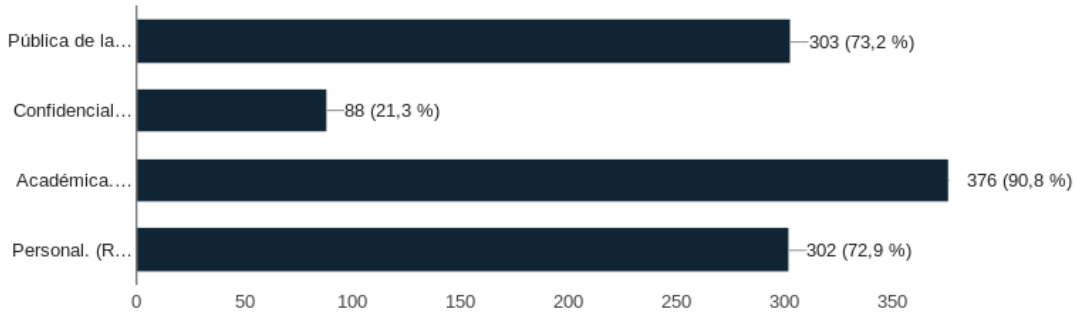

Figure 8.2.10: ¿Qué clase de información maneja en la Universidad?

Análisis: En esta pregunta se complementa la clasificación de la información basada en la muestra tomada, 414 usuarios de la universidad, la cual fue:

Pública: Un 73,2% usa información que está disponible al público, como lo es la mostrada en las páginas web de los dominios de la universidad.

Confidencial: Hay un porcentaje de 21,3% que usa información confidencial de la universidad, que su divulgación no autorizada podría tener un impacto grave a ésta.

Académica: Como es de esperarse es el tipo de información más alta manejan los usuarios, el resultado fue 90,8%.

Personal: Un conjunto grande utiliza información personal en la universidad, como lo es sobre redes sociales, correos, cuentas bancarias, entre otras. Un 72,9% fue el resultado.

10. ¿Es consciente de los riesgos a los que se expone usted con el uso de éstas tecnologías tanto dentro como fuera de la universidad?

- Sí.
- No.

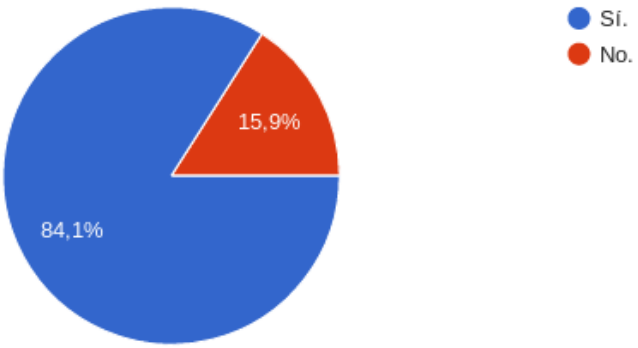

Figure 8.2.11: ¿Es consciente de los riesgos?

Análisis: Un 84,1% de los usuarios dice ser consciente de los riesgos a los que se está expuesto con el uso de estas tecnologías dentro y fuera de la universidad; mientras un 15,9% dice no serlo.

11. ¿Está enterado de prácticas o recomendaciones de seguridad informática y de la información que se hayan socializado en la Universidad (como folletos informativos de seguridad)?:

- Sí.
- No.

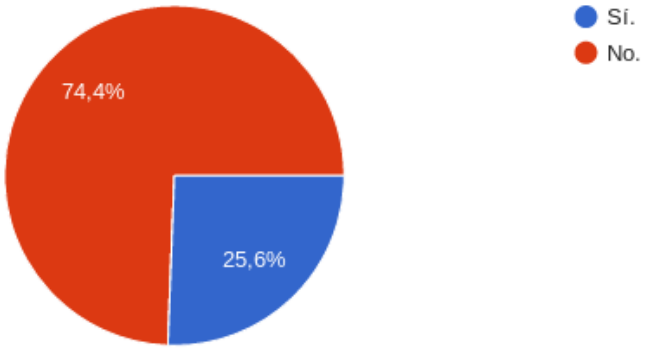

Figure 8.2.12: ¿Está enterado de prácticas o recomendaciones de seguridad informática y de la información que se hayan socializado en la Universidad?

Análisis: Un 74,4% no está enterado de prácticas o recomendaciones de seguridad informática y de la información, que se divulguen en la universidad. Un 25,6% afirma estarlo.

12. ¿Cuenta usted con alguna guía en la universidad que le permita el acceso y manejo seguro de éstas tecnologías para no ser víctima de un fraude informático?

- Sí.
- No.

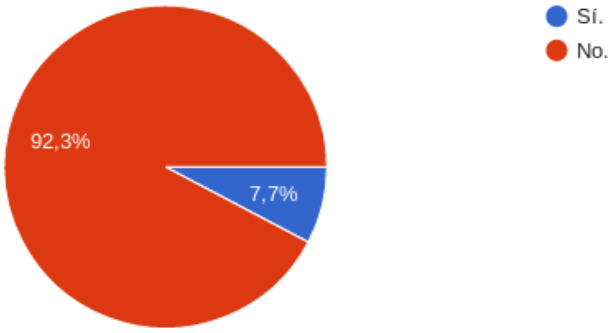

Figure 8.2.13: ¿Cuenta usted con alguna guía en la universidad que le permita el acceso y manejo seguro de éstas tecnologías?

Análisis: Un 92,3% no cuenta con una guía o recomendación en la universidad para tener un uso seguro de las recursos TI. Un 7.7% afirma tenerla.

13. **¿Qué opina sobre la seguridad informática y de la información en la Universidad del Valle?:**

- Buena.
- Regular.
- Mala.

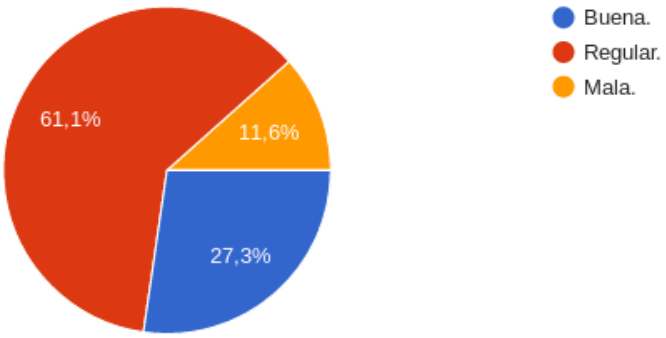

Figure 8.2.14: ¿Qué opina sobre la seguridad informática y de la información en la Universidad del Valle?

Análisis: Un 27,3% afirma que la seguridad informática y de la información en la universidad es buena; un 61,1% dice que es regular; y que es mala, un 11,6%.

8.3 Análisis de la entrevista a la OITEL

La entrevista permitida al Director a cargo de la OITEL, Oficina de Informática y Telecomunicaciones, da fe de su responsabilidad a cargo de "la custodia de los datos que están en los sistemas de información y de todas las aplicaciones institucionales" como obligación estipulada por el Estado.

Actualmente la Universidad cuenta con unas políticas de seguridad y gestión de la información del año 2008 elaboradas mediante una consultoría, pero reitera que "se requiere un apoyo para poderlas actualizar a la realidad de hoy". Por lo tanto, determina que la Universidad sí ansía y debe ir un paso adelante en el tema de la seguridad informática y de la información; tal es el nuevo proceso de consultoría que se llevará a cabo pronto para la instauración de un SGSI en su sistema, para la actualización de las políticas.

La OITEL brinda capacitaciones en materia de seguridad de la información a través de tres canales:

1. RUAV (Red Universitaria de Alta Velocidad): La cual brinda capacitaciones a los miembros de la Red, entre ellos a la Univerisdad del Valle [65].

2. NotiRed: Boletin que tiene como objetivo brindar información práctica y útil a la comunidad universitaria acerca de los servicios, proyectos y desarrollos de la Red Institucional de Transmisión de Datos de la Universidad del Valle [66].

3. Esfuerzos propios con el coordinador de Infraestructura, realizados a través de dos charlas al año.

8.4 Sugerencias

En vista de los resultados obtenidos se plantean las siguientes sugerencias respecto a la información deducida de las actividades de investigación:

1. Realizar campañas de sensibilización para fomentar una buena educación base a los usuarios de la universidad respecto a la importancia de la seguridad informática y de la información; pues debido a la intervención tecnológica en la mayoría de campos de estudio y trabajo en la universidad, es necesario conocer la importancia del manejo seguro de estas tecnologías en las carreras universitarias con las que tienen relación. Así, los porcentajes de una nueva muestra con los mismos objetivos podría relucir un aumento en la cultura de seguridad de la información. Campañas específicas como por ejemplo el manejo de contraseñas, el uso de antivirus y mecanismos de protección para los computadores de los usuarios, las actualizaciones periódicas de los computadores de los usuarios, información sobre vulnerabilidades recientes en el área de seguridad informática para que sea divulgada a los usuarios.

2. Proponer capacitaciones a los miembros de la universidad; por ejemplo a los estudiantes, que pueda ser dictada una capacitación en la temática en los inicios de todos los semestres, puede aplicarse igualmente a los trabajadores.

9

Protocolo de buenas prácticas

Este protocolo ayuda en el esfuerzo por proveer una guía útil para los profesionales que operen con sistemas de información, sus empleados y demás miembros de la universidad que deseen implementar buenas prácticas de seguridad informática y de la información:

1. Generar una Toma de conciencia por parte de toda la comunidad de la organización educativa con respecto a la importancia de la seguridad de la información. Para esto los encargados de la administración de los sistemas deben enviar a los usuarios las respectivas medidas de seguridad que deben ejercer para poder realizar cada uno su labor adecuadamente y evitar así el incremento de amenazas a las que esté expuesta la información en la universidad como la personal. Esto también aplica para los usuarios de la universidad que no hagan parte de los sistemas de información, pues igualmente hacen parte de otros sistemas dentro de la comunidad; es necesario brindar recomendaciones sobre la importancia de la seguridad de la información en sus tareas diarias si hacen uso de alguna tecnología informática propia o de la universidad. Para esto se deja propuesto una política de seguridad para la universidad y se destaca un ejemplo de campaña para promover la cultura de seguridad informática.

2. Solicitar un acompañamiento normativo en el proceso en el que se haga participe de un sistema de información, y donde este activo sea de carácter confidencial y requiera que se le brinde las apropiadas medidas de seguridad. Es decir, si el usuario hace parte de un sistema donde los datos intercambiados dentro de este son de alto riesgo para la comunidad universitaria y no se brinda una apropiada gestión de seguridad, entonces deben acudir a que sea establecido un acompañamiento normativo de parte de la dirección; o en lo más próximo el usuario debe solicitar una guía adecuada para brindarle

seguridad al proceso que necesita llevar a cabo dentro de la Universidad.

3. Vigilar que la toma de conciencia sea llevada a cada proceso importante de la universidad que repercuta a el uso de tecnologías informáticas y sistemas de información, es decir, hacer las veces de auditor y monitorear que los datos son tratados de forma segura y no se evidencian fallas de seguridad; esto con la finalidad de apuntar a dejar un pie adelante para realizar de manera oportuna consultorías, para apuntar a una certificación. Esto se logra con el PROPORCIONAMIENTO DE BUENAS PRÁCTICAS debidamente divulgado a todos los miembros de la institución. Aplica igualmente para cada usuario de la universidad, ya que éste debe estar en la capacidad de asegurar que hace uso adecuado de las tecnologías informáticas con las que tenga contacto y así mismo debe tener cierta periodicidad para buscar y encontrar malas pŕacticas de seguridad informática que realice acordes a las recomendaciones facilitadas por los administradores de sistemas; además están en la obligación de informar sobre fallos en el sistema a sus respectivos administradores si estos no han sido informados.

A continuación se explica cada paso del protocolo y las mejores medidas para lograrlo.

9.1 Toma de conciencia

Los usuarios deberían ser conscientes de la necesidad de la seguridad de la información en los sistemas de información y lo que pueden hacer para mejorarla dentro de la Universidad. Según una guía de seguridad de los sistemas de información y redes [67] propuesta por OECD (The Organisation for Economic Co-operation and Development, en español Organización para la Cooperación y el Desarrollo Económicos), la cual es una entidad de cooperación internacional, compuesto por 35 estados, cuyo objetivo es coordinar sus políticas económicas y sociales; afirma que se deben tener en cuenta los puntos a continuación para la toma de conciencia en lo que a la seguridad de la información respecta:

1. Tener consciencia de los riesgos y las medidas de seguridad disponibles es la primera línea de defensa para la seguridad de los sistemas y redes de información.

2. Los sistemas de información y las redes pueden verse afectados por riesgos tanto internos como externos.

3. Los usuarios deben entender que los fallos de seguridad pueden dañar significativamente los sistemas y redes bajo su control o con los que estén relacionados.

4. Los usuarios de TI deben ser conscientes de la configuración y las actualizaciones disponibles de sus sistemas, su lugar dentro de las redes, las buenas prácticas que pueden implementar para mejorar la seguridad y las necesidades de otros participantes. Los usuarios comunes, que no tienen autorización de realizar estas revisiones o no saben cómo proceder por carentes conocimientos de informática, están en la obligación de solicitar el acompañamiento de la oficina de informática si se evidencian malas configuraciones o comportamientos que puedan perjudicar la seguridad de la información de sistemas propios o de la universidad.

Para el cumplimiento de este propósito se plantea el difundir desde pequeñas recomendaciones de

seguridad hasta una guía apropiada para algunos casos en específico donde exista una necesidad de acogimiento de la seguridad informática y de la información. Como ejemplo, a continuación se cita la campaña de concientización de seguridad informática y de la información de la Universidad de Harvard [68]; a continuación se presenta un objetivo que promueve la campaña:

Uso de contraseñas fuertes:

- *Crear contraseñas que sean únicas y difíciles de adivinar.*
- *Usar verificación en dos pasos cuando este método esté disponible.*

Una contraseña es la manera de probar que eres tú. La tecnología ha continuado mejorando cada vez más, ¿no es tiempo de mejorar la manera de manejar las contraseñas? Lee los apartados presentes a continuación para ayudarte a crear una contraseña fuerte, controlar tus demás contraseñas en un gestor de contraseñas, y habilitar la verificación en dos pasos para prevenir el robo de cuentas. *¿Cómo crear una contraseña fuerte?.*

Contraseñas a evitar:

¿Hace uso de algunas de estas contraseñas o la combina con alguna palabra del diccionario? Si es así, entonces necesita actualizar su contraseña a una más fuerte.

1. Año con cuatro dígitos: 19XX, 20XX, otros aniversarios o años famosos como 1776 o 1066.

2. "password": pass, password, p@$$word o alguna variante.

3. Referencias de deportes: footballfan, hockey, gosox.

4. Nombres: De Mascotas, cónyuges, hijos, nietos, celebridades.

5. Información personal: Su nombre, dirección de correo electrónico, número de teléfono o número de seguro social.

6. Patrones de teclado o secuencias: qwerty, asdf, 123456,abc123.

Buenas contraseñas

Una buena contraseña deberá tener los siguientes requerimientos:

1. Un carácter en mayúscula (A-Z).

2. Un carácter en minúscula (a-z).

3. Un número (0-9) y/o símbolos (tales como !, # o %)

Una manera puede ser empezando con una palabra que recuerdes: pamphlet. Luego le agregas algunos de los elementos mencionados anteriormente, quedando: pAMPh$3let

Algo mejor - Frases de contraseñas o Passphrases

Son más largas y complejas que las contraseñas. Son más fáciles de recordar, pero más difíciles de adivinar.

1. Método A: Convierte una frase en un acrónimo

Escoge una frase que puedas recordar y extrae las primeras letras de cada palabra.

Mccic:Iiig,web? -> Mint chocolate chip ice cream: If it isn't green, why even bother?

2. Método B: Cuatro palabras al azar

Utilice un diccionario grande o un generador de palabras aleatorio para seleccionar sus palabras. La contraseña debe tener al menos 20 caracteres. Escribir mal una palabra, capitalizar o agregar puntuación puede agregar algo de fuerza adicional.

Ej: FloorBrightAlreadySoemthing9 ó rubbishconsiderGREEENSwim3.

Lo mejor - Gestores de contraseñas

Las contraseñas más fuertes son creadas por gestores de contraseñas, un software que genera y mantiene un registro de contraseñas complejas y únicas para todas sus cuentas. Todo lo que tienes que recordar es la contraseña del gestor de contraseñas. Al elegir, elija uno que admita la verificación en dos pasos. Harvard proporciona a todos los miembros de su comunidad un gestor de contraseñas llamado LastPass [69].

Puntos a resaltar sobre las contraseñas:

1. Privacidad por favor: Mantén tus contraseñas de manera privada y no las compartas con nadie. Los centros de soporte nunca te preguntarán por tu contraseña por teléfono o email.

2. ¿Cómo administrarlas?: Tienes docenas de cuentas, y eso significa que necesitas decenas de contraseñas seguras. Afortunadamente, hay aplicaciones para ayudarle a realizar un seguimiento de ellos. Un gestor de contraseñas le ayudará a crear, usar y almacenar contraseñas fácilmente.

3. No reutilizar: Usar la misma contraseña para todas sus cuentas es muy arriesgado. Si su cuenta en cualquier servicio está comprometida, todas sus cuentas se ponen en riesgo. Utilice una contraseña única para cada cuenta.

4. Hazlo mejor: Cuando habilita la verificación en dos pasos, cada vez que utilice su cuenta en un dispositivo nuevo, aparecerá un código de autorización en su teléfono. Sin el código, un ladrón de contraseñas no puede tomar el control de su cuenta. Es la mejor manera de proteger su cuenta de los ciberdelincuentes. La verificación en dos pasos está disponible para Twitter, Facebook, Google y otros.

Campañas de este tipo pueden ser incentivadas por cualquier usuario de la universidad que tenga una propuesta para mejorar la seguridad informática y de la información, en vista de los resultados de la encuesta a una parte de la comunidad, de los que la mayoría anotaron que no es buena.

9.2 Acompañamiento normativo

Es necesario que el usuario de la Universidad del Valle que haga uso de las TI tenga en cuenta que es indispensable el seguimiento de las normas que permiten la gestión de la seguridad informática y de la información. Para esto es recomendable incentivar la toma de la norma ISO/IEC 27001[7] al hablarlo en reuniones con la dirección Universitaria, dado el caso que las TI y los sistemas de información implicados representen una gran importancia para el/los usuario(s). Si es incentivada en la Universidad, se lograría encaminar la acreditación para al menos uno de los procesos dentro de la Universidad; lo cual

sería una visión a alcanzar y mantener con el paso del tiempo, que apuntaría a mejorar la seguridad de la información presente en la organización educativa.

Para esclarecer cómo la implantación de la norma se llevaría a cabo para un proceso dentro de la Universidad, según una lista de apoyo[70] publicada por Dejan Kosutic, experto en la normativa, afirma que se debe:

1. Obtener el apoyo de la dirección encargada del sistema de información.

Es uno de los principales causantes del fracaso de la imposición de la norma ISO/IEC 27001; fundamentalmente por motivos económicos e insuficientes recursos humanos para trabajar en el proyecto.

2. Utilizar una metodología para gestión de proyectos.

Es necesario que el acogimiento de la norma se tome como parte de un gran proyecto, puesto que es necesario involucrar muchas personas que son actores principales del proceso de formación del SGSI; no obstante, esto puede tomar bastante tiempo y es necesario contar con una metodología.

3. Definir el alcance del Sistema de gestión de la seguridad de la información.

Es necesario establecer la normativa iniciando desde un proceso o a una parte de la organización institucional; ya que es una entidad grande.

4. Redactar una política de alto nivel sobre seguridad de la información.

Es el documento más importante en su SGSI, el cual no es muy específico pero si debe contener temás básicos de la seguridad de la información de la Universidad. Se recomienda seguir los lineamientos de la ISO/IEC 27001 [7].

5. Definir la metodología de evaluación de riesgos.

Es la tarea que más trabajo requiere en el acopio de los requerimientos de la norma. Define las reglas para identificar los activos, las vulnerabilidades, las amenazas, las consecuencias y probabilidades, como también el nivel aceptable de riesgo.

6. Realizar la evaluación y el tratamiento de riesgos.

Aquí se implementa lo anteriormente planeado dentro de la organización, para obtener una visión integral de los peligros sobre la información de la organización educativa.

7. Redactar la declaración de aplicabilidad.

Luego de realizar el tratamiento de riesgos se conocerá qué controles de referencia serán utilizados y cuales no, los objetivos que se lograrán con estos y su implementación.

8. Redactar el plan de tratamiento de riesgos.

Aquí se amplía la documentación del tratamiento en donde se define claramente como se implementarán los controles.

9. Definir la forma de medir la efectividad de sus controles y de su SGSI.

Se debe medir el cumplimiento de los objetivos del SGSI como también el logro de los objetivos de cada control en la declaración de aplicabilidad.

10. Implementar todos los controles y procedimientos necesarios

Es la tarea de mayor riesgo puesto que implica la toma de nuevas tecnologías, pero sobre todo la

adaptación de nuevas conductas en la organización; y es de gran riesgo puesto que los usuarios pueden resistirse al cambio, para lo cual es de vital importancia la siguiente tarea.

11. Implementar programas de capacitación y concienciación

Esto con la finalidad de explicarle a los usuarios la importancia de optar por acoplar las nuevas políticas y procedimientos; además de brindar una capacitación correcta para el eficiente funcionamiento en el SGSI.

12. Realizar todas las operaciones diarias establecidas en la documentación de su SGSI.

Esto le compete a la organización para realizar registros diarios al haberse adaptado en la normativa. Teniendo de esta manera cómo ver que las tareas de los usuarios se están realizando según lo estipulado.

13. Monitorear y medir su SGSI.

Aquí se debe verificar que los resultados que obtiene cumplan con lo que se estableció en los controles de riesgo; de no cumplirse se deben tomar medidas correctivas y/o preventivas.

14. Realizar la auditoría interna.

Estas auditorías deben llevarse a cabo con la finalidad de descubrir fallas en el sistema por muy pequeñas que puedan ser; para así, dejar activas medidas correctivas y/o preventivas. Se recomienda orientarse bajo la normativa ISO 19011:2011 sobre la auditoría de los sistemas de gestión, incluidos los principios de auditoría, gestión de un programa de auditoría y realización de auditorías de sistemas de gestión.

15. Realizar la revisión por parte de la dirección.

"La dirección no tiene que configurar el cortafuegos", es decir, los usuarios miembros de la dirección de la universidad deben saber qué está sucediendo en el SGSI; es decir, en base a los resultados obtenidos la dirección debe seguir tomando decisiones importantes para mejorar la seguridad de la información en el proceso evaluado.

16. Implementar medidas correctivas.

La norma exige que se identifique oportunamente la raíz de una no conformidad y haya una solución y control.

En el artículo publicado por Nadia Mumtaz sobre el Análisis de la seguridad de la información a través del manejo de activos en los institutos académicos de Pakistan[71], la política establecida para el manejo de los activos de una institución educativa debe constar de otra serie de políticas propuestas por la ISO/IEC 27001:

Responsabilidad de los activos

La propuesta de está política tiene como objetivo administrar los activos (Véase capítulo 6.3.6.4) importantes de la institución e implementar los controles apropiados. De la misma manera cada activo identificado debe tener un propietario que será el responsable por él. Este objetivo puede lograrse mediante:

Listado de activos

Todos los activos deben ser identificados y mantener en una lista de inventario. Cada detalle menor

sobre el activo debe ser mencionado en la lista de inventario. El activo puede ser de cualquier tipo:

1. Activos de información: Incluye información en bases de datos o archivos de datos, información de investigaciones, documentación de procesos operativos, documentación de sistemas, contratos o acuerdos, materiales de capacitación.

2. Activos de software: Incluye ambos, aplicaciones y sistemas de información del software.

3. Activos físicos: Incluye dispositivos informáticos y de comunicaciones, como también medios de almacenamiento.

4. Servicios de apoyo como HVAC (Heating, ventilation and air conditioning - Calefacción, ventilación y aire acondicionado), iluminación y suministro de energía.

5. Información personal de empleados, profesores, estudiantes y autoridades superiores.

6. Activos como reputación e imagen de la organización.

7. Información de ubicación lógica o física de cada activo.

8. Información sobre copias de seguridad.

Asignación del propietario de activos

Cada tipo de información y activos relacionados con instalaciones de procesamiento de información deben tener un dueño. Los controles son:

1. El propietario de cada activo es responsable de la clasificación y confidencialidad de la información.

2. El propietario debe revisar periódicamente el control de acceso del activo.

Uso de los activos

Se debe definir, documentar e implementar el direccionamiento de políticas con el uso de los activos y las instalaciones de procesamiento de la información. Los controles son:

1. Procedimiento / directrices definidos para el uso aceptable de los activos.

2. Procedimientos y directrices para el uso de sistemas residentes.

3. Procedimientos y guías para dispositivos portátiles y no portátiles que se utilizan de forma remota.

4. Procedimientos definidos para la toma de conciencia.

Clasificación de la información

Toda la información en la universidad debe ser clasificada de acuerdo a:

Categorías

Pública: Puede ser visto por cualquier persona en el mundo, Ej: de contactos importantes, los nombres. Direcciones de correo electrónico, números de teléfono, anuncios de las autoridades, publicaciones, comunicados de prensa, información del curso, etc.

Abierta: Todos los miembros del Instituto pueden tener acceso a la información, Ej: contactos importantes, los nombres. Direcciones de correo electrónico, números de teléfono. Comunicaciones aprobadas Ej: Noticias, actualizaciones de la universidad, políticas, procedimientos y procesos.

Confidencial: Algunos miembros específicos pueden ver la información con la autorización apropiada o en base a una necesidad de saber, Ej: Información específica para un departamento, Información de Identidad Universitaria (Carnet), Datos de contrato de empleados, Documentos en formato de bor-

rador.

Altamente confidencial: Se da acceso a un número reducido de miembros, Ej: Datos bancarios (números de cuenta), datos financieros, registros médicos, calificaciones de estudiantes, Exámenes, documentos de investigación en curso, servidores, salas de servidores, nombres de usuario y contraseñas, investigaciones, procedimientos disciplinarios, entre otros.

Secreta: Solo la alta dirección autorizada de la universidad puede acceder a esta información secreta o el usuario al que se le haya concedido acceso autorizado por parte de la alta dirección. Ej: Copias de seguridad o backups, datos financieros seleccionados, información de contratos con los proveedores, proyectos de investigación seleccionados, Documentación de los planes de proyectos futuros de la Universidad, los activos de información seleccionados estrictamente confidenciales también pueden pertenecer a esta categoría.

Guía para la clasificación

La información y las instalaciones de procesamiento de información deben clasificarse en términos de valor o requisitos legales. Los controles son:

1. Definición de la responsabilidad del propietario del activo.
2. Revisión de la gestión de activos para asegurar que las clasificaciones mantengan la CIA(Confidentiality, Integrity and Availability - en español, Confidencialidad, Integridad y Disponibilidad) de la información y de los sistemas de procesamiento de información.

Etiquetado y manejo

La información debe ser etiquetada y manejada adecuadamente por el propietario de acuerdo a su categoría.

1. La información en todos los formularios y medios (lógicos y físicos) debe etiquetarse y manejarse en consecuencia.
2. Procedimientos documentados para mantener la cadena de custodia de la información.

9.3 Validación del protocolo y proporcionamiento de buenas prácticas de seguridad informática y de la información

Esta parte reúne las acciones y mecanismos a través de los cuales el protocolo propone unas prácticas de seguridad informática y de la información aplicadas a los casos de estudio de las vulnerabilidades que se expondrán, para incentivar el aseguramiento de la información o recursos expuestos en la Universidad del Valle. En la Tabla 9.3.1 se realiza un breve esbozo de las vulnerabilidades o fallas detectadas en la Universidad por inspección física y digital como miembro de la comunidad basándome en los ejemplos de vulnerabilidades de la ISO/IEC 27005[59]; luego de esto se detalla el proceso de aplicación del protocolo por cada punto.

Vulnerabilidad	Tipos	Amenazas
Exposición de información personal (cédulas) en dominios públicos de la Universidad.	Personal, Organización	Desprestigio, abuso de los derechos y error en el uso.
Acceso sin restricción a cuenta de usuario y revelación de información personal en un sistema de información	Software, Personal, Organización	Abuso de los derechos, error en el uso, falsificación de derechos, mal funcionamiento del software, modificación de funcionalidades permitidas por el sistema e ingeniería social aplicada a la información expuesta.
Exposición de contraseñas de usuarios en un sistema de información sin la debida protección.	Software, Personal, Organización	Suplantación de identidad a través de ingeniería social mediante las contraseñas de usuarios, falsificación de derechos, hurto de información confidencial y delitos informáticos.

Table 9.3.1: Esbozo de algunas vulnerabilidades de la Universidad del Valle

9.3.1 Aplicación del protocolo

Se menciona a continuación de manera detallada los riesgos por cada vulnerabilidad y las conductas propuestas a seguir mediante el protocolo.

1. *Exposición de información personal en dominios públicos de la universidad*

El número de identificación personal asignado por la Registraduría General de la Nación, como lo puede ser el número de cédula, corresponde a un dato público de acuerdo con el artículo 213 del Código Electoral[72]. Por lo cual, para el tratamiento de dicho dato no se hace necesario contar con la autorización del titular del mismo, sin embargo se debe tener en cuenta que pese a que no se requiera autorización sí se debe dar cumplimiento a las demás disposiciones de la Ley 1581 de 2012 [73], entre ellas, los deberes y principios para el tratamiento de datos personales. La publicación que llevan a cabo las entidades públicas de los contratos que suscriben se encuentra ampliamente justificada en un deber que la ley le ha impuesto a las mismas y tiene como finalidad el desarrollo de principios de rango constitucional. Es decir, a pesar de que el número de cédula es un dato "público" a no ser que el usuario, o estudiante en este caso, haya autorizado expresamente a que la universidad lo publique en un servidor que se comparte abiertamente, esta incurriendo en violación de la ley de datos personales.

Además de evidenciar un claro desprestigio para las personas que figuran en el dominio con sus cédulas, esta información pública pone en riesgo de demanda por mal manejo de datos personales y puede terminar en un punto pivote para el robo de identidad del usuario (estudiante, profesor, empleado, etc).

Por lo tanto el protocolo toma como objeto de estudio en este caso, los administradores de sistemas encargados de publicar dicha información en el dominio público de la universidad.

Toma de conciencia: Debe verse divulgado el riesgo de robo de identidad, a los usuarios administradores y responsables de la publicación del contenido que contiene información sensible de los

usuarios de la universidad, puesto que están haciendo público información como la cédula, y la adquisición de esta podría permitir junto con el nombre obtener una fotocopia de la cédula no autenticada y por ahí se empieza.

Acompañamiento normativo: Los encargados de administrar la publicación de aquella información hacen parte de un sistema de información y es necesario que al haber sido informados de los riesgos a los que se someten al publicar información indebida, para mejorar estos comportamientos deben guiar sus procesos acorde a una normativa para mejorar la seguridad informática y de la información, para esto se recomienda la ISO/IEC 27001 [7].

Práctica de seguridad: Debe realizarse una correcta segmentación de la información, es decir, pensar bien quién necesita ver qué, cómo y cuando. Para este caso debe excluirse la cédula y la información sensible adyacente al contenido publicado. Desde la perspectiva de una analista externo, la única información que se debería divulgar sería el nombre; puesto que esta información que yace en el dominio de la universidad tiene finalidades académicas.

2. *Acceso sin restricción a cuenta de usuario y revelación de información personal*

El sistema de información expuesto permite ingresar solamente con el código del estudiante, a partir de ahí las funcionalidades del sistema de información están disponibles. Permitiría realizar modificaciones en el sistema con el código únicamente y además la información es expuesta y puede ser utilizada para ataques de ingeniería social.

Toma de conciencia: Debe ser sensibilizada la importancia de la seguridad informática a los usuarios administradores y la dirección encargada del desarrollo del sistema de información para que puedan ser planteadas mejores soluciones de acceso al sistema, en vista del funcionamiento que presenta. Por lo tanto esta concientización se logra si se expone los riesgos de ataques de ingeniería social a los encargados del sistema y se debe optar por un seguro control de acceso de usuarios al sistema de información.

Acompañamiento normativo: No obstante una política de seguridad para el seguro control de acceso al sistema de información debe ser propuesta y llevada a cabo para el cumplimiento de la seguridad de la información, esto se logra si el sistema ve ligado su comportamiento a los estándares correctos de seguridad que proporcionen la protección contra el riesgo de que la información expuesta no comprometa un usuario de la universidad por un ataque de ingeniería social.

Práctica de seguridad: Los encargados de la gestión del sistema deben discutir la solución recomendable para evitar esta vulnerabilidad y una posible alternativa es la asignación de contraseña al usuario que ingresa.

3. *Exposición de contraseñas de usuarios en un sistema de información sin la debida protección.*

Este sistema permite el ingreso del usuario solicitándole la contraseña. Hasta ahí todo va en orden. La vulnerabilidad empieza cuando al usuario se le olvida la contraseña, pues debe acudir al administrador para que este le permita el ingreso al sistema. El usuario solicita el soporte del administrador y este le

dice en palabras la contraseña que olvidó, además de escribírsela en un papel para que le sea visible, aquí se tiene la vulnerabilidad expuesta.

Toma de conciencia: El SSO (System Security Officer, en español el jefe de seguridad del sistema) es el encargado de la administración de la seguridad del sistema, para este caso en particular el SSO debe ser capacitado debidamente sobre los riesgos de la exposición de contraseñas que está generando el sistema y las amenazas que pueden tomar partido de ello [74].

Acompañamiento normativo: Una política de seguridad informática y de la información en la universidad debería encargarse del problema de la exposición de contraseñas, dictaminando las responsabilidades de un SSO y el manejo seguro de contraseñas para los sistemas de información.

Práctica de seguridad: Es necesario usar algoritmos de encriptación para las contraseñas, con la finalidad de que éstas no sean expuestas por ningún canal y el SSO debe estar en la capacidad de permitirle el cambio de la contraseña sin tener registro de las ya usadas.

Para finalizar el protocolo se adjunta esta sección de recomendaciones para ser tenidas en cuenta en pro del afianzamiento de la seguridad informática y de la información; uno de los puntos recalca la importancia de la protección de los datos y sugiere unos pasos para este objetivo, dada la naturaleza del ataque del ransomware del que múltiples usuarios escucharon o se dieron cuenta por la popularidad de la noticia.

9.4 Recomendaciones

Esta parte del protocolo propone cultivar múltiples buenas prácticas de seguridad informática y de la información para los usuarios de la universidad y permitir que administradores de sistemas de información supervisen la seguridad de los activos de información, asegurándose de que cada usuario actúa bajo estas prácticas. La sensibilización en materia de seguridad informática debe llevarse a cabo como un programa continuo para garantizar que la capacitación y el conocimiento no se acaba de entregar como una actividad anual, sino que se utiliza para mantener un alto nivel de conciencia de seguridad sobre una base diaria.

El objetivo principal recae en recrear la toma de conciencia a través de programas de capacitación que envuelva a toda la comunidad universitaria, para lo cual se puede empezar por brindar materiales de entrenamiento disponibles para todas las áreas de la organización, que pueden haber sido desarrollados de manera interna, adaptados del trabajo de una organización profesional o comprados a un proveedor. Hay muchos proveedores que brindan materiales bien preparados a través de la web. La finalidad es capacitar a los miembros en temas relacionados a la ciberseguridad, como lo es el uso obligatorio de contraseñas seguras, evitar ataques de *social engineering* o ingeniería social, evitar descargar código malicioso, etc.

El programa de entrenamiento debe requerir que el personal reconozca haber recibido y comprendido el contenido que se entrega. Esto es crucial para el éxito del programa creado para generar con-

ciencia sobre la ciberseguridad. Si el contenido se entrega y no se entiende, el usuario puede, sin darse cuenta, poner en riesgo la información de la organización o la información personal igualmente. Los comentarios sobre el contenido y la comprensión del entrenamiento son fundamentales para asegurar que el usuario entienda el contenido y las buenas prácticas de seguridad de la organización.

Otra consideración importante para la inclusión en la formación de seguridad informática a tener en cuenta según el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) o PCI DSS, es la conciencia de los ataques de ingeniería social[75], en el que indican que una forma en que un atacante puede utilizar la ingeniería social es adquiriendo las credenciales de un usuario y trabajar su camino a través de la organización de un área de baja seguridad a un área de alta seguridad. Adaptar esta conciencia para reflejar los tipos de ataques que la organización puede encontrar proporciona resultados más efectivos. Los usuarios deben ser conscientes de los métodos comunes por los cuales los estafadores, hackers u otras personas malintencionadas pueden tratar de obtener credenciales, datos de tarjetas de pago y otros datos confidenciales; esto para minimizar el riesgo de que el usuario divulgue información confidencial a personas externas. También se recomienda la capacitación en políticas, cuando éstas ya sean implementadas, y procedimientos organizacionales que especifiquen el manejo adecuado de los datos, incluyendo el intercambio y transmisión de datos sensibles.

9.4.1 Recomendaciones generales de buenas prácticas de seguridad informática y de la información

Como buenas prácticas a tomar se especifican algunas medidas de seguridad que son tomadas y adaptadas de recomendaciones realizadas por:

- Miembros de la RedIRIS, red española para Interconexión de los Recursos Informáticos de las universidades y centros de investigación, en su documento de recomendaciones de seguridad[76].
- Datto, compañía que ofrece soluciones de respaldo de información [77].

9.4.1.1 Recomendaciones generales

En este apartado se destacan aspectos generales para mejorar la seguridad informática en las instituciones educativas:

- Adaptar políticas de seguridad de la información, puesto que muchas organizaciones educativas no las tienen establecidas para especificar los derechos o las sanciones en las que pueden incurrir los usuarios con el uso de las tecnologías informáticas de la universidad.
- Definir un responsable para el área de seguridad informática, o un correo al que se pudieran enviar notificaciones de seguridad y así mismo tener retroalimentación.

- Implementar controles de acceso y de respuestas a incidentes informáticos para mitigar los ataques de denegación de servicios y barridos de puertos y redes hacia otras localizaciones que provienen de aulas o espacios de uso compartido dentro de las instituciones.

9.4.1.2 Otras recomendaciones

En vista de la popularidad del *Ransomware,* se presentan a continuación soluciones a optar para una mejor protección cibernética ya que muchos de los equipos de computo de la Universidad operan en Windows.

- Conducir una evaluación de los riesgos de la seguridad informática. Entender las posibles amenazas (ej: el tiempo determinado de un Ransomware y el impacto que puede tener en los procesos de negocio de la organización(pérdida de ingresos). Usar esta información para modelar una estrategia de seguridad acorde a sus necesidades.

- Entrenar a los usuarios, puesto que las amenazas cibernéticas están en constante crecimiento. Esto debe incluir ejemplos de amenazas como también instrucciones en mejores prácticas de seguridad (ej: bloquear los computadores al alejarse de su sitio de trabajo)

- Proteja su red y sus dispositivos. Implementar una directiva de contraseñas que requiere contraseñas seguras que caducan cada 90 días. Implementar tecnologías de cortafuegos, VPN y antivirus para garantizar que la red y los puntos finales no sean vulnerables a ataques. Considere implementar la autenticación multifactor. El monitoreo continuo de la red también debe considerarse esencial. Cifrar unidades de disco duro.

- Mantenga el software actualizado. Es esencial utilizar productos de software actualizados y estar atento a la gestión de parches. Los delincuentes cibernéticos explotan vulnerabilidades de software usando una variedad de tácticas para obtener acceso a computadoras y datos. La OITEL no puede garantizar la actualización de su *laptop*, tampoco el control de un celular que se conecte a la red. Por ende, si usted como usuario se entera de un parche de seguridad necesario y urgente como lo fue el reportado por Microsoft para evitar la vulnerabilidad que exponía el WannaCry, debe sugerir a la OITEL actualice dicho equipo de trabajo interno de la universidad; dado que la OITEL no maneje unas buenas políticas de actualización, y esto pondría en tela de juego la seguridad de la información no solo del equipo sino de la universidad, por ser parte de ésta.

- Cree políticas directas de ciberseguridad. Escribir y distribuir un conjunto claro de reglas e instrucciones sobre prácticas de seguridad cibernética para los empleados. Esto variará de un proceso a otro, pero puede incluir políticas de uso de redes sociales, de traer su propio dispositivo, requisitos de autenticación, etc.

- Haga una copia de seguridad de sus datos. Las copias de seguridad diarias son un requisito para recuperarse de la corrupción o pérdida de datos como resultado de infracciones de seguridad. Considere la posibilidad de utilizar una herramienta de protección de datos moderna que realiza copias de seguridad periódicas de datos periódicamente durante todo el día para evitar la pérdida de datos. *Sugerencia:* En la Universidad del Valle se ofrece el almacenamiento ilimitado en Google Drive con el que podría realizar la copia de seguridad de sus datos. Otras herramientas para usuarios con más conocimiento en informática se recomienda:

  - BackupPC (*Open Source*)[78].
  - Duplicati (*Open Source*)[79].
  - ownCloud (*Open Source*)[80].
  - StoreOnce de la empresa HP (Hewlett-Packard)[81].
  - Datacastle [82].
  - Acronis [83].

- Controlar el acceso a las computadoras. Utilice tarjetas llave o medidas de seguridad similares para controlar el acceso a las instalaciones, y asegúrese de que los empleados utilicen contraseñas seguras para ordenadores portátiles y de escritorio. Los privilegios administrativos sólo deben darse al personal de TI de confianza. En la universidad esto aplicaría de tal manera que sea propuesta y generada un política de seguridad de acceso a los equipos de cómputo y otra política para el uso de contraseñas seguras.

Entre estas soluciones se reitera la importancia que tiene la implantación de políticas de seguridad informática y de la información en la universidad, para todos sus miembros: tanto sus empleados, como estudiantes. Como lo define la Universidad de Economía de Praga, República Checa, en sus reglas de operación del sistema de información IS VSE[84], que tiene en su subdivisón a los otros subsistemas de la Universidad; empero, el alcance de sus reglas se dispone para todos los empleados, estudiantes, entidades que lleven a cabo actividades dentro de la institución, como a todos sus miembros; actores de su sistema. En base a lo mencionado anteriormente, las políticas de seguridad no pueden ser generadas por un usuario, deben ser socializadas con la alta dirección de la universidad y propuestas con un plan estratégico de control sobre los objetivos de la seguridad de la información, el cual requiere de presupuesto y personal especializado en el área de seguridad de la información, como los encargados de la gestión de riesgo.

10
Conclusiones

Muchos aspectos de la vida cotidiana dependen de Internet y de las computadoras, incluyendo las comunicaciones (correo electrónico, teléfonos celulares, mensajes de texto), transporte (señales de control de tráfico, sistemas de motores de automóviles, navegación de aviones), gobierno (registros de nacimiento / muerte, seguridad social, registros), finanzas (cuentas bancarias, préstamos, cheques electrónicos), medicina (equipo, registros médicos) y educación (aulas virtuales, boletines de calificaciones en línea, investigación). Considere qué cantidad de información personal se almacena en su computadora o en el sistema de otra persona. ¿Cómo se mantienen seguros los datos y los sistemas en los que residen (o se transmiten) esos datos?. El aumento del volumen y la sofisticación de las amenazas de seguridad cibernética, incluyendo la identificación de estafas de phishing, robo de datos y otras vulnerabilidades en línea, exigen que permanezcamos vigilantes sobre la seguridad de nuestros sistemas e información.

Fue un gran reto haber escogido un campo de estudio que en la universidad no se destaca, como lo es la seguridad informática. Esto es inferido por la falta de esta área de estudio en la universidad como también por los problemas encontrados al inicio de la investigación, mencionados a continuación:

- Falta de tutores con experticia en el área en la universidad.
- Poca documentación en trabajos de grado de la universidad en la temática.
- El acuerdo de confidencialidad que impedía llegar más a fondo en la investigación.
- La falta de preeminencia en la temática por parte de varios participantes en las encuestas a los administradores de los sistemas.

- Falta de políticas internas en cuanto a la prioridad de la seguridad de la información y temas relacionados, así sea una prioridad secundaria por ser tesis de un estudiante, se asume que la cantidad de trabajo no permite dar prioridad a estas campañas en la oficina de informática.

El protocolo fue diseñado a medida que proseguía la investigación, y la metodología desde el inicio del proyecto fue planteada con la finalidad de esperar que los resultados de los mecanismos utilizados aportaran a la formación de mejores propuestas en el protocolo. El retraso por disponibilidad de la oficina de informática impidió armar el prototipo del protocolo en base a los resultados, es decir, el alcance se vio reducido por la burocracia de la universidad; pese a esto, se logró en últimas instancias medir los resultados, analizarlos y realizar deducciones que aportaran al protocolo, con ayuda de los analistas externos que tienen pericia en el campo de estudio. Los resultados de las encuestas, quedan para ser usados en propuestas a la OITEL para atacar cada uno de los problemas derivados, se hizo sugerencias en la sección. Las proposiciones realizadas en la aplicación del protocolo en los casos de estudio analizados y vistos como vulnerabilidades de la universidad, pretenden ser acogidas en la menor cantidad de tiempo posible después de llegar a oídos de la oficina de informática. De no ser así, la información que sigue estando expuesta, pone en riesgo a los usuarios de la universidad. Usuarios que pueden pasar a víctimas de delitos informáticos, por ello es necesario que se tomen medidas; es claro que la información personal como la cédula, y otros datos personales proporcionados por un sistema de información y una exposición de contraseñas generan una mezcla con la que un delito informático mayor es posible.

El desarrollo del trabajo de grado se vio influenciado significativamente por la decisión de optar por la rama de la seguridad informática en el campo de las ciencias de la computación, alentado por profesores de la universidad que resaltaban la importancia de esta área a lo largo de la carrera universitaria, como también por la influencia de expertos que ya llevan algunos años de experiencia en la industria de la seguridad informática y de la información. Así pues, este proyecto permitió adquirir múltiples habilidades por la capacitación brindada por los tutores y logró que éstas se pusieran en práctica, como lo fue el caso de la identificación de algunas vulnerabilidades y la instrucción en los estándares de la seguridad de la información para observar los posibles riesgos y amenazas en los sectores estudiados dentro del alcance del proyecto. Por lo tanto, se sostiene que la seguridad de la información puede ser protegida y manejada si se toma en consideración una cultura de seguridad de la información eficaz y los empleados son capaces de reconocer, conocer y manejar sus propias percepciones para asegurar sus activos en la organización.

11
Trabajo futuro

Como trabajo a futuro se propone:

- Instaurar un Sistema de Gestión de Seguridad de la Información en procesos o sistemas de información en algún departamento de la universidad.
- Promover la formación académica en materia de seguridad informática, que se podría empezar por abrir una rama de estudio en la carrera de ingeniería de sistemas, pues es necesaria para áreas como el desarrollo de software.
- Alcanzar la visión de fomentar la implantación de un departamento de seguridad informática y de la información en la universidad, no dejar centralizado este proceso en la OITEL.
- Realizar más consultorías en los demás departamentos de la universidad, que no sean solo en la OITEL.
- Realizar cursos continuos o proyectos que ayuden a capacitar a todos los usuarios de la universidad.

Bibliografía

[1] OITEL - Oficina de Informática y Telecomunicaciones, "Políticas para el uso de los recursos informáticos." http://www.univalle.edu.co/politicainformatica/. [En línea; accedido 2016-11-27].

[2] Foursys, "The Top 5 Cybersecurity mistakes made in Education." https://www.foursys.co.uk/gated-assets/Top_5_Cybersecurity_mistakes_made_in_Education.pdf. [En línea; accedido 2017-04-22].

[3] Paolo Passeri, "February 2017 Cyber Attacks Statistics." http://www.hackmageddon.com/category/security/cyber-attacks-statistics/. [En línea; accedido 2017-03-07].

[4] Symantec Corporation, "Internet Security Threat Report." https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf. [En línea; accedido 2017-04-22].

[5] NovaInfosec, "Cyber Security versus Information Security." https://www.novainfosec.com/2014/05/05/cyber-security-versus-information-security/.

[6] J. R. S. Agustín López Neira, "El portal de ISO 27001 en Español." http://www.iso27000.es/sgsi.html, 2005. [Online; accessed 2016-02-20].

[7] "Information Technology. Security Techniques. Information Security Management Systems. Requirements.," standard, International Organization for Standardization, Geneva, Mar. 2013.

[8] Microsoft, "The security risk management guide." http://trygstad.rice.iit.edu:8000/Books/TheSecurityRiskManagementGuide-Microsoft.pdf. [En línea; accedido 2017-01-15].

[9] G. Allison, "The ministry of defence saw spike in cyber-security breaches last year, the government has confirmed.," *UK Defence Journal*, 2017. [En línea; accedido 2017-02-07].

[10] L. Kleinrock, "An internet vision: the invisible global infrastructure," *Ad Hoc Networks*, vol. 1, no. 1, pp. 3 – 11, 2003.

[11] B. Dupont, "L'évolution du piratage informatique: De la curiosité technique au crime par sous-traitance»," *AAPI (Éd.), Le respons@ ble*, vol. 2, pp. 63–81, 2010.

[12] S. Abiteboul, "Vers une nouvelle science des risques?," *Risques*, 2013.

[13] H. Zou, "Protection of personal information security in the age of big data," in *Computational Intelligence and Security (CIS), 2016 12th International Conference on*, pp. 586–589, IEEE, 2016.

[14] IIROC, "Cybersecurity best practices guide." http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf. [En línea; accedido 2017-08-20].

[15] A. Da Veiga, "The influence of information security policies on information security culture: illustrated through a case study," 2015.

[16] Y. Hou, P. Gao, and B. Nicholson, "Understanding organisational responses to regulative pressures in information security management: the case of a chinese hospital," *Technological Forecasting and Social Change*, 2017.

[17] C. Joshi and U. K. Singh, "Information security risks management framework–a step towards mitigating security risks in university network," *Journal of Information Security and Applications*, vol. 35, pp. 128–137, 2017.

[18] SecurityScorecard, "Higher education security report." https://cdn2.hubspot.net/hubfs/533449/2015_Higher_Education_Security_Report.pdf. [En línea; accedido 2017-05-24].

[19] J. P. Rey, L. Corrons, M. García, and A. Ramírez, "Reportaje, wannacry, la penúltima gran amenaza," *Ctrl: control & strategias*, no. 646, pp. 38–41, 2017.

[20] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, "The role of cyber-security in information technology education," in *Proceedings of the 2011 conference on Information technology education*, pp. 113–122, ACM, 2011.

[21] R. Elliott *et al.*, "Information security in higher education. professional paper series,# 5.," 1991.

[22] S. C. B. U. news, "Top university under 'ransomware' cyber-attack." http://www.bbc.com/news/education-40288548. [En línea; accedido 2017-07-17].

[23] M. Balduzzi, V. Ciangaglini, and R. McArdle, "Targeted attacks detection with spunge," in *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on*, pp. 185–194, IEEE, 2013.

[24] W. C. Banks, "Cyber espionage and electronic surveillance: Beyond the media coverage," *Emory LJ*, vol. 66, p. 513, 2016.

[25] R. A. Clarke and R. K. Knake, *Cyber war*. Tantor Media, Incorporated, 2014.

[26] Y. Hollander, "Prevent web site defacement," *Internet Security Advisor*, vol. 3, no. 6, p. 22, 2000.

[27] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "Ddos attack detection method using cluster analysis," *Expert Systems with Applications*, vol. 34, no. 3, pp. 1659–1665, 2008.

[28] R. Droms and W. Arbaugh, "Authentication for dhcp messages," tech. rep., 2001.

[29] J. Cook, H. Wu, and L. Foster, "Dns server access control system and method," Nov. 1 2005. US Patent 6,961,783.

[30] R. Baloch, *Ethical hacking and penetration testing guide*. CRC Press, 2014.

[31] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Longman Publishing Co., Inc., 2003.

[32] E. S. Raymond, "How to become a hacker," *Database and Network Journal*, vol. 33, no. 2, pp. 8–9, 2003.

[33] M. Manion and A. Goodrum, "Terrorism or civil disobedience: toward a hacktivist ethic," *ACM SIGCAS Computers and Society*, vol. 30, no. 2, pp. 14–19, 2000.

[34] N. Provos *et al.*, "A virtual honeypot framework.," in *USENIX Security Symposium*, vol. 173, pp. 1–14, 2004.

[35] I. S. Winkler and B. Dealy, "Information security technology? don't rely on it. a case study in social engineering.," in *USENIX Security Symposium*, vol. 5, pp. 1–1, 1995.

[36] G. Buehrer, B. W. Weide, and P. A. Sivilotti, "Using parse tree validation to prevent sql injection attacks," in *Proceedings of the 5th international workshop on Software engineering and middleware*, pp. 106–113, ACM, 2005.

[37] X. Xing, W. Meng, B. Lee, U. Weinsberg, A. Sheth, R. Perdisci, and W. Lee, "Understanding malvertising through ad-injecting browser extensions," in *Proceedings of the 24th International Conference on World Wide Web*, pp. 1286–1295, International World Wide Web Conferences Steering Committee, 2015.

[38] I. Santos, Y. K. Penya, J. Devesa, and P. G. Bringas, "N-grams-based file signatures for malware detection.," *ICEIS (2)*, vol. 9, pp. 317–320, 2009.

[39] D. Spruson and N. Ferguson, "Intellectual property management: A practical guide for electrical and electronics related industries," 2007.

[40] P. Hautrive, "Les protocoles réseaux." http://hautrive.free.fr/reseaux/architectures/protocoles-de-reseaux.html. [En línea; accedido 2017-01-18].

[41] J. S. Broderick, "Isms, security standards and security regulations," *information security technical report*, vol. 11, no. 1, pp. 26–31, 2006.

[42] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decision support systems*, vol. 15, no. 4, pp. 251–266, 1995.

[43] D. Fink and G. Disterer, "International case studies: To what extent is ict infused into the operations of smes?," *Journal of Enterprise Information Management*, vol. 19, no. 6, pp. 608–624, 2006.

[44] D. M. Chess and S. R. White, "An undetectable computer virus," in *Proceedings of Virus Bulletin Conference*, vol. 5, 2000.

[45] British Standards Institution, "ISO 27001 History." http://www.british-assessment.co.uk/iso-27001-history/. [En línea; accedido 2016-11-20].

[46] L. Charlet, "ISO Survey 2015." https://www.iso.org/the-iso-survey.html, 2015. [Online; accessed 2017-04-20].

[47] IT Governance, "ISO 27001 Global Report 2016." https://www.itgovernance.co.uk/download/ISO27001-Global-Report-2016.pdf. [En línea; accedido 2017-01-27].

[48] Ryerson University, "Information Protection Policy - Ryerson Policies and Procedures." http://www.ryerson.ca/policies/administration/informationprotectionpolicy/. [Online; accessed 2017-01-22].

[49] Harvard University, "Information Security Policy - Harvard University." https://policy.security.harvard.edu/. [En línea; accedido 2016-12-07].

[50] McGill University, "Politique relative au bon usage des ressources informatiques de McGill." https://www.mcgill.ca/secretariat/files/secretariat/responsible-use-of-mcgill-it-policy-on-the-french.pdf. [En línea; accedido 2017-01-21].

[51] L. Charlet, "ISO Survey 2015." https://security.harvard.edu/use-strong-passwords. [Online; accessed 2017-02-25].

[52] Universidad ICESI, "Política de seguridad de la información." http://www.icesi.edu.co/manuales/servicios_apoyo/images/Infraestructura/PoliticaSeguridadInformacion.pdf. [En línea; accedido 2016-12-20].

[53] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security*, vol. 38, pp. 97–102, 2013.

[54] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research*, vol. 20, no. 1, pp. 79–98, 2009.

[55] W. L. McGill, "Defensive dissuasion in security risk management," in *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*, pp. 3516–3521, IEEE, 2009.

[56] W. Lee and D. Xiang, "Information-theoretic measures for anomaly detection," in *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on*, pp. 130–143, IEEE, 2001.

[57] L. M. Galan, "Un modelo formal para la especificación, análisis, verificación e implantación de protocolos de seguridad." 1998.

[58] Y. Marrero Travieso, "La Criptografía como elemento de la seguridad informática.," *ACIMED*, vol. 11, 12 2003.

[59] "Information Technology. Security Techniques. Information Security Risks Management.," standard, International Organization for Standardization, Geneva, Mar. 2011.

[60] N. Evans and J. Price, "Responsibility and accountability for information asset management (iam) in organisations," ACI-Academic Conferences International, 2014.

[61] M. Alotaibi, S. Furnell, and N. Clarke, "Information security policies: A review of challenges and influencing factors," in *Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for*, pp. 352–358, IEEE, 2016.

[62] R. Kissel, "Glossary of key information security terms (nist ir 7298, revision 1), 205. national institute of standards and technology (nist), 2011."

[63] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (isra)," *Computers & Security*, vol. 57, pp. 14–30, 2016.

[64] C. Seale, "Quality in qualitative research," *Qualitative inquiry*, vol. 5, no. 4, pp. 465–478, 1999.

[65] Asociación Red Universitaria de Alta Velocidad del Valle del Cauca – RUAV, "¿Qué es RUAV?." http://ruav.edu.co/que-es-ruav/?tab=que_es_ruav. [En línea; accedido 2017-05-31].

[66] Oficina de Informática y Telecomunicaciones – OITEL, "NotiRed: Red-es tu ayuda." http://notired.univalle.edu.co/. [En línea; accedido 2017-05-31].

[67] OECD (Organisation De Coopération Et De Développement Economiques), "Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité." https://www.oecd.org/sti/ieconomy/15582260.pdf. [En línea; accedido 2017-04-10].

[68] Harvard University - Information Security, "Information Security Awareness Campaign." https://security.harvard.edu/smallactions. [En línea; accedido 2017-02-14].

[69] LastPass, "Harvard and LastPass." https://lastpass.com/harvard/. [En línea; accedido 2017-02-14].

[70] D. Kosutic, "Lista de apoyo para implementación de ISO 27001." https://advisera.com/27001academy/es/knowledgebase/lista-de-apoyo-para-implementacion-de-iso-27001/. [En línea; accedido 2016-12-21].

[71] N. Mumtaz, "Analysis of information security through asset management in academic institutes of pakistan," in *2015 International Conference on Information and Communication Technologies (ICICT)*, pp. 1–4, Dec 2015.

[72] R. nacional del estado civil, "Código electoral colombiano." http://aceproject.org/ero-en/regions/americas/CO/colombia-decreto-2241-de-1986-codigo-electoral/at_download/file. [En línea; accedido 2017-08-20].

[73] A. de Bogotá, "Ley estatutaria 1581 de 2012," *Recuperado de http://www. alcaldiabogota. gov. co/sisjur/normas/Norma1. jsp*, 2012.

[74] S. L. Brand, *Password Management Guideline: Department of Defense*. DIANE Publishing, 1985.

[75] PCI Security Standards Council, "Best Practices for Implementing a Security Awareness Program." https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf. [En línea; accedido 2017-04-21].

[76] Chelo Malagón Poyato, Francisco Monserrat Coll, David Martínez Moreno, "Recomendaciones de seguridad." https://www.rediris.es/cert/doc/docu_rediris/recomendaciones/recomendaciones.pdf. [En línea; accedido 2016-12-21].

[77] Total Data Protection Platform- Datto, "The Essential Cybersecurity Toolkit for SMBs." http://somerbysit.co.uk/wp-content/uploads/2017/05/Datto_Essential_Cybersecurity_Toolkit_3.pdf. [En línea; accedido 2017-05-22].

[78] "Backuppc." http://backuppc.sourceforge.net/. [En línea; accedido 2017-08-20].

[79] "Duplicati, free backup software to store encrypted backups online for windows, macos and linux." https://www.duplicati.com/. [En línea; accedido 2017-08-20].

[80] "owncloud, a safe home for all your data." https://owncloud.org/. [En línea; accedido 2017-08-20].

[81] "Hpe storeonce data protection backup appliances." https://www.hpe.com/us/en/storage/storeonce.html. [En línea; accedido 2017-08-20].

[82] "Mobile data protection and analytics." http://datacastlered.com/. [En línea; accedido 2017-08-20].

[83] "Acronis backup 12.5." https://www.acronis.com/es-mx/. [En línea; accedido 2017-08-20].

[84] RNDr. Karel Nenadál (Director of the computing center), "Pravidla provozování a využívání univerzitního informačního systému Vysoké školy ekonomické v Praze (Rules for operation and use of the university information system of the University of Economics in Prague (PR 08/2011))." https://www.vse.cz/predpisy/doc/343_20150429_105337.pdf?dt=20170528. [En línea; accedido 2017-04-30].