Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Industrial

PLAN PARA ELABORAR POLÍTICAS DE SEGURIDAD DE INFORMACIÓN PARA UN DEPARTAMENTO DE TECNOLOGÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Juan Eliú Pacheco Morán
Asesorado por el Ing. Renaldo Girón Alvarado

Guatemala, septiembre de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PLAN PARA ELABORAR POLÍTICAS DE SEGURIDAD DE INFORMACIÓN PARA UN DEPARTAMENTO DE TECNOLOGÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JUAN ELIÚ PACHECO MORÁN
ASESORADO POR EL ING. RENALDO GIRÓN ALVARADO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO INDUSTRIAL

GUATEMALA, SEPTIEMBRE DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Narda Lucía Pacay Barrientos
VOCAL V	Br. Walter Rafael Véliz Muñoz
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

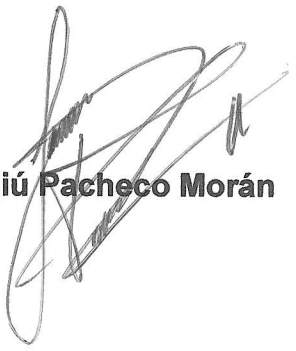
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADORA	Inga. Miriam Patricia Rubio Contreras de Akú
EXAMINADOR	Ing. Edwin Giovanni Tobar Guzmán
EXAMINADOR	Ing. Mynor Armando Dardón Díaz
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PLAN PARA ELABORAR POLÍTICAS DE SEGURIDAD DE INFORMACIÓN PARA UN DEPARTAMENTO DE TECNOLOGÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Mecánica Industrial, con fecha 19 de agosto de 2009.



Juan Eliú Pacheco Morán

Universidad De San Carlos De Guatemala
Facultad De Ingeniería
Escuela de Ingeniería Mecánica Industrial

Guatemala, Agosto de 2015

Ing. César Urquizú
Director Escuela de Ingeniería Mecánica Industrial
Pte.

Estimado Ingeniero Urquizú:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante: **Juan Eliú Pacheco Morán**, quien se identifica con carné universitario 1996-16207 y DPI 1938749890608, extendido en Chiquimulilla, Santa Rosa. Dicho trabajo de graduación se titula: "**PLAN PARA ELABORAR POLÍTICAS DE SEGURIDAD DE INFORMACIÓN PARA UN DEPARTAMENTO DE TECNOLOGÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**", el cual he tenido a la vista y he revisado suficientemente, considerando que reúne las condiciones y características necesarias para poder ser avalado por la Escuela de Ingeniería Mecánica Industrial y continuar con su proceso de aprobación como trabajo de tesis.

Sin otro particular,

Atentamente:

Ing. Renaldo Girón Alvarado
COLEGIADO 5977

Msc. Ing. **Renaldo Girón Alvarado**
Colegiado No. **5977**

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF.REV.EMI.117.015

Como Catedrático Revisor del Trabajo de Graduación titulado **PLAN PARA ELABORAR POLÍTICAS DE SEGURIDAD DE INFORMACIÓN PARA UN DEPARTAMENTO DE TECNOLOGÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,** presentado por el estudiante universitario **Juan Eliú Pacheco Morán,** apruebo el presente trabajo y recomiendo la autorización del mismo.

"ID Y ENSEÑAD A TODOS"

INGA. KARLA MARTÍNEZ
Colegiada 5,706

Ing. Karla Lizbeth Martínez Vargas
Catedrático Revisor de Trabajos de Graduación
Escuela de Ingeniería Mecánica Industrial

Guatemala, agosto de 2015.

/mgp

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF.DIR.EMI.160.015

El Director de la Escuela de Ingeniería Mecánica Industrial de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el Visto Bueno del Revisor y la aprobación del Área de Lingüística del trabajo de graduación **PLAN PARA ELABORAR POLÍTICAS DE SEGURIDAD DE INFORMACIÓN PARA UN DEPARTAMENTO DE TECNOLOGÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,** presentado por el estudiante universitario **Juan Eliú Pacheco Morán**, aprueba el presente trabajo y solicita la autorización del mismo.

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARL
DIRECCION
Escuela de Ingeniería Mecánica I
FACULTAD DE INGENIE

Ing. César Ernesto Urquizú Rodas
DIRECTOR
Escuela de Ingeniería Mecánica Industrial

Guatemala, septiembre de 2015.

/mgp

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.446-2015

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Industrial, al trabajo de graduación titulado: **PLAN PARA ELABORAR POLÍTICAS DE SEGURIDAD DE INFORMACIÓN PARA UN DEPARTAMENTO DE TECNOLOGÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,** presentado por el estudiante universitario: **Juan Eliú Pacheco Morán,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, septiembre de 2015

/cc

ACTO QUE DEDICO A:

Dios	Esa fuerza poderosa que nos da el ser y nos guía durante el arduo camino de nuestras vidas.
La Universidad de San Carlos de Guatemala	Porque en sus aulas aprendí a valorar el verdadero sentido de ser un profesional para servirle al país con dignidad y honestidad.
Mis padres	Juan Pacheco (q. e. p. d.) y Camelia Morán de Pacheco, ese par de ángeles que con muchos desvelos, incalculables esfuerzos, mucho amor y comprensión me han guiado sabiamente para alcanzar todas mis metas. Infinitas gracias, los amo.
Mis hermanos	Romin, Sohemia y Olfi (q. e. p. d.) y Sarita Pacheco, Maribel y Marlyn Ambeliz, Felipe Zamora y Rodolfo Morán. Soporte y comprensión para los tiempos difíciles y buena compañía para los ratos felices. Los llevo en mi corazón.
Mi esposa	Flory Marisol Monterroso Peralta, apoyo incondicional y cariño en todo momento para alcanzar las metas propuestas.

Mi hijo Juan Diego Pacheco Monterroso, una de las muchas y buenas razones que tengo para seguir adelante con mis sueños. Te amo hijito.

Mi tía Aura Esperanza Ambeliz, por su valiosa ayuda, apoyo y comprensión.

Mis primas Dailin y Emeli Cruz, por su cariño y aliento en todo momento. Y por compartir esta meta alcanzada. Espero que mi triunfo sea un ejemplo para que puedan alcanzar también sus metas profesionales.

Mis amigos Abner Aguilar, Marvin Juárez, Sergio González, Luis Méndez, William Rodríguez, Lester Padilla, Obdulio Madriles, Víctor Pérez, Nahum Aroche, Maru López, Tono Tojín, Nery De León, Emilio Monterroso, Edgar Rodas, Karel Díaz, Darcy Huertas, Oscar Jiménez y todos los compañeros del DPD, que a lo largo de la carrera me apoyaron, me aconsejaron y compartieron penas y alegrías.

Mi asesor Ingeniero Renaldo Girón Alvarado, quien con su ayuda desinteresada me apoyó para culminar este trabajo de graduación.

Mi exjefe Ing. Jorge Gómez Méndez, por permitirme elaborar este trabajo y por su apoyo en el DPD.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Activo Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Antivirus Programa que tiene como finalidad detectar y eliminar virus informáticos, así como, proteger los equipos de otros programas peligrosos conocidos genéricamente como malware.

Ataque Evento, exitoso o no, que atenta sobre el buen funcionamiento de un sistema informático.

Autenticación Procedimiento de comprobación de la identidad de un usuario como medida de seguridad frente a posibles operaciones fraudulentas a través de la Red.

Certificado digital	También llamado certificado de clave pública, es un documento electrónico que usa una firma electrónica para atestiguar que una clave pública pertenece a una persona u organismo concreto.
Criptografía	La criptografía es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta irreconocible e ilegible para todo aquel que no conozca el sistema mediante el cual ha sido encriptado, haciendo indescifrable el contenido de la información que no conozca la forma de descifrar el criptograma.
CSIRT	Equipo de Respuesta ante Emergencias Informáticas, del inglés (*Computer Security Incident Response Team*) es un equipo de respuesta a incidentes de seguridad de información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.
Contingencia	Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Firewall

Un cortafuegos (*firewall* en inglés) es una parte de un sistema o una red que está diseñado para bloquear o denegar el acceso a personas no autorizadas a una computadora o a una red de computadoras, permitiendo al mismo tiempo comunicaciones autorizadas.

HTTP

Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de comunicaciones en Internet, es el protocolo más utilizado.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) (en español: Protocolo de transferencia de Hipertexto seguro) es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en Internet, generalmente para transacciones de pagos o cada vez que se intercambie información sensible, por ejemplo, claves, número de tarjetas de crédito, etcétera.

Ícono

En el campo de la informática, un ícono es un pequeño gráfico en pantalla que identifica y representa a algún objeto (programa, comando, documento o archivo), usualmente con algún simbolismo gráfico para establecer una asociación.

Impacto	Medir la consecuencia al materializarse una amenaza.
Internet	Es una red informática descentralizada, que para permitir la conexión entre computadoras opera a través de un protocolo de comunicaciones. Para hacer referencia a ella además se utiliza el término Web en inglés, refiriéndose a una tela de araña para representar esta red de conexiones.
IP	(*Internet Protocol*, Protocolo de Internet). Es una dirección basada en un número compuesto de 4 cifras, cada una entre 0 y 254, la cual se usa para identificar a un equipo dentro de una red que utiliza el protocolo de comunicación IP.
LDAP	Siglas del inglés *Lightweight Directory Access Protocol* (en español Protocolo Ligero de Acceso a Directorios) habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etcétera). A manera de síntesis, es un protocolo de acceso unificado a un conjunto de información sobre una red.

Navegador	Es una aplicación que opera a través de Internet, interpretando la información de archivos y sitios web para que se pueda leer.
Plan de negocios	El plan de negocios es un documento que ayuda al empresario a analizar el mercado y planificar la estrategia de un negocio.
POA	Siglas de Plan Operativo Anual, es un documento formal en el que se enumeran y describen de forma general, por parte de los responsables en una institución, los objetivos y metas que se pretenden alcanzar durante un año laboral.
RADIUS	Siglas del inglés *Remote Authentication Dial In User Service* (en español: Servidor Remoto de Autenticación Telefónica de Usuario). Es un protocolo AAA (Autenticación, Autorización y Administración) para aplicaciones de redes o movilidad IP.
Riesgo	Es la probabilidad de que suceda la amenaza o evento no deseado.
Sistemas factor 2	Sistema de autenticación, donde el usuario debe validar 2 factores: algo que sabe (usuario y *password*) y algo que posee (por ejemplo, una credencial almacenada en un dispositivo).

SMS	(*Short Message Service*), Servicio de mensajes cortos, es un sistema para enviar mensajes de texto vía teléfonos celulares, a los cuales se les conoce comúnmente como mensajitos.
Tecnófoba	Término utilizado en informática para describir a una persona que rechaza, tiene cierto temor o resistencia al cambio en relación a la tecnología.
Vulnerabilidad	Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

RESUMEN

Una política de seguridad de información debe ser analizada, estructurada y plasmada para divulgarse y hacerse del conocimiento de los colaboradores de la institución, esto con el fin de lograr que todos estén enterados y comprometidos con las directrices de la misma.

Para un Departamento Tecnológico, como el que se trata en este documento, es de suma importancia crear un plan para elaborar políticas de seguridad de información, esto con el fin de hacer el esquema de análisis de la situación actual, los pormenores de la implementación de dicha política y la metodología que se utilizará para darle seguimiento y mantener el sistema funcionando para que éste se vaya mejorando con la realimentación que se obtendrá de los problemas que se vayan resolviendo y documentando durante la puesta en marcha de la política.

El recurso humano por sobre todos los demás componentes, es al que se le debe poner especial cuidado, ya que su participación, compromiso y lealtad hacia la institución, será uno de los pilares más importantes para llevar a cabo un plan y que éste se consolide a través del tiempo y se convierta en una tarea ordinaria para todos, para así lograr, que la política de seguridad de información cumpla su fin principal: el aseguramiento de la información, que es uno de los activos más importantes que poseen las instituciones hoy en día.

OBJETIVOS

General

Elaborar un plan de políticas de seguridad de información para un Departamento de Tecnología de la Universidad de San Carlos de Guatemala.

Específicos

1. Determinar el alcance de las políticas de seguridad.

2. Determinar el riesgo.

3. Identificar objetivos de control y controles.

4. Definir estándares y procedimientos para implementar las políticas.

5. Definir cómo se implementarán las políticas.

6. Definir responsabilidades y roles para darle cumplimiento a las políticas.

7. Establecer los métodos y procedimientos para darle seguimiento a las políticas propuestas.

INTRODUCCIÓN

Los sistemas de gestión especialmente en los aspectos de seguridad, generalmente no son considerados con la seriedad que merecen en el ámbito empresarial guatemalteco, pero no cabe duda que lo serán en muy corto plazo.

Para un Departamento de Tecnología constituye una etapa fundamental y visionaria, la formulación de políticas de seguridad para la información, para con ello, garantizar alta disponibilidad y confiabilidad de sus productos y servicios a los clientes internos como externos, así como, encaminar un área tan importante como es la informática y las telecomunicaciones, hacia un futuro donde los servicios de tecnología de la institución sean más competitivos y con mayor fiabilidad.

Dichas políticas para seguridad de información se formulan con base en las políticas generales de la organización y con las directrices específicas en cuanto a tecnología de la información se refiere, para con ello, administrar aspectos como la prevención y corrección de problemas relacionados con pérdida o corrupción de información, ya que la información es un bien muy importante por ser la base del funcionamiento de las empresas modernas a través del intercambio y manipulación electrónica de la misma.

Un Departamento de Tecnología debe fijar sus objetivos y metas basado en los volúmenes de datos que maneja, el equipo con que manipulará los mismos, así como, los recursos económicos, humanos y tecnológicos que dispone para diseñar mejores estrategias para protección de la información.

1. ANTECEDENTES GENERALES

1.1. La Universidad de San Carlos de Guatemala

Es la única universidad estatal en Guatemala, fundada en el siglo XVII, actualmente es el ente rector de la educación superior en el país, así como, la difusión de la cultura en todas sus manifestaciones.

La Universidad de San Carlos de Guatemala (también conocida y llamada por sus siglas: USAC) es la universidad más grande y antigua de Guatemala, siendo además la única estatal. Establecida en el Reino de Guatemala durante la colonia española, fue la más prestigiosa institución de educación superior de Centro América y la única de Guatemala hasta 1954.

1.1.1. Historia

La Universidad de San Carlos se fundó por Real Cédula de Carlos II de España, el 31 de enero de 1676.

Los estudios a nivel superior inician desde mediados del siglo XVI, cuando el primer obispo de Guatemala, Lic. Francisco Marroquín, funda el Colegio Universitario de Santo Tomás, en 1562, para becados pobres; se inició con las cátedras de filosofía, derecho y teología. Los bienes del colegio universitario se usaron un siglo más tarde para conformar el patrimonio de la Universidad de San Carlos, junto con los bienes que legó para fundarla, el señor correo mayor Pedro Crespo Suárez.

Desde principios del siglo XVI otros colegios, como Santo Domingo y San Lucas, obtuvieron licencia temporal de conferir grados.

También hubo estudios universitarios desde el siglo XVI, tanto en el Colegio Tridentino como en Colegio de San Francisco, aunque no otorgaron grados. La Universidad de San Carlos adquirió categoría internacional. Al ser declarada Pontificia por la Bula del Papa Inocencio Xl, emitida el 18 de junio de 1 687. Además de cátedras de su tiempo: derecho civil y canónico, medicina, filosofía y teología, incluyó la docencia de lenguas indígenas.

Durante la colonia, cruzaron sus aulas más de 5 000 estudiantes y de las doctrinas escolásticas, se enseñó filosofía moderna y pensamiento científico inglés y francés del siglo XVIII. Sus puertas se abrieron a todos: criollos, españoles, indígenas y entre sus primeros alumnos graduados se pueden encontrar nombres indígenas y personas de humilde cuna.

Uno de los más ilustres nombres que se pueden mencionar en relación a la academia y su aporte a la historia de Guatemala es el sacerdote Franciscano José Antonio Liendo y Goicoechea, quién reformó la educación en la Universidad de San Carlos y también fue profesor de todos los líderes de la Independencia de Centroamérica.

Las opiniones de Fray José Antonio Liendo y Goicoechea, tanto políticas como filosóficas, fueron duramente rebatidas por los escolásticos. Entre sus obras destaca la dedicada a cómo erradicar la mendicidad en la región de Guatemala.

Figura 1. **Fray José Antonio Liendo y Goicoechea**

Fuente: Diálogos Revista Electrónica de Historia. http://bit.ly/1JShl5w . Consulta: abril de 2015.

Los concursos de oposición para catedráticos también datan desde aquella época y en muchos de ellas triunfaron guatemaltecos humildes, tal es el caso del Doctor Tomás Pech y el Doctor Manuel Trinidad de Avalos y Porres, a quien se atribuye la fundación de la investigación científica en Guatemala, por la evidencia que existe en sus trabajos médicos experimentales, como transfusiones e inoculaciones en animales.

Se contempló en la legislación desde sus fases iniciales, la discusión académica, el comentario de textos, los cursos monográficos y la lección magistral. Se ordena la libertad de criterio en sus estatutos, que exigen el conocimiento de doctrinas filosóficas opuestas a la dialéctica, para que el esfuerzo de la discusión beneficiara la educación universitaria.

La necesidad de una reforma pedagógica y lograr cambios en los criterios científicos, es también una característica que data de los primeros años de la universidad. Fray Antonio de Goicoechea fue precursor de ellas.

En las ciencias jurídicas, cuyo estudio comprendía derecho civil y canónico, se registraron modificaciones importantes al incorporar el examen de derecho civil y romano, así como, derecho de gentes, cuya introducción se remonta al siglo XVIII. También, se crearon cátedras de economía política y letras.

La Universidad de San Carlos de Guatemala ha contado también, desde sus primeros años, con representantes que el país recuerda con orgullo: el doctor Felipe Flores sobresalió con inventos y teorías, que se anticiparon a muchas de ulterior triunfo en Europa. El doctor Esparragoza y Gallardo puede considerarse un magnífico exponente de la cirugía científica y en el campo de derecho, el doctor José María Álvarez, autor de las renombradas Instituciones de Derecho Real de Castilla y de Indias, publicadas en 1818.

Los primeros signos de colegiación pueden observarse desde 1810, cuando se fundó el ilustre Colegio de Abogados, cuyo fin principal era la protección y depuración del gremio. Esta institución desapareció casi a finales del siglo XIX, para resurgir en 1947. Semejante a lo ocurrido en otros países de América, la universidad luchó por su autonomía, que había perdido a fines del siglo pasado y la logró el 9 de noviembre de 1944, decretada por la Junta Revolucionaria de Gobierno.

Con ello, se restableció el nombre tradicional de la Universidad de San Carlos de Guatemala y se le asignaron fondos para lograr un respaldo económico estable.

La Constitución Política de Guatemala emitida de 1945, consagró como principio fundamental la autonomía universitaria y el Congreso complementó las disposiciones de la Carta Magna con la emisión de una Ley Orgánica para la Universidad, así como, una Ley de Colegiación obligatoria para todos sus egresados que ejerzan su profesión en el país.

Desde septiembre de 1945, la universidad funciona como entidad autónoma con autoridades elegidas por un cuerpo electoral, conforme a preceptos legales establecidos en su Ley Orgánica; y se ha normado por los siguientes principios que, entre otros, son producto de la Reforma Universitaria de 1944: libertad de elegir autoridades y personal docente o ser electo para dichos cargos sin injerencia del Estado.

La asignación de fondos que se manejan por el Consejo Superior Universitario con entera autonomía, se derivan de un aporte constitucional, el cual se encuentra establecido en la Constitución Política de República de Guatemala en su Artículo 84, donde establece que a la Universidad de San Carlos de Guatemala le corresponde una asignación no menor al 5 por ciento del Presupuesto General de Ingresos Ordinarios del Estado.

Aparte de ello, se le concedió libertad administrativa y ejecutiva para que trabaje de acuerdo con las disposiciones del Consejo Superior Universitario. Dotación de patrimonio consistente en bienes registrados a nombre de la universidad. Elección de personal docente por méritos propios, con base a un examen de oposición, participación de estudiantes en elecciones de autoridades. Participación de profesionales catedráticos o no, en las elecciones de autoridades.

1.1.2. Ubicación

La Universidad de San Carlos de Guatemala, está ubicada en la zona 12 de la ciudad capital de Guatemala, en la denominada ciudad Universitaria, su ubicación exacta está en latitud 14,5887537º, longitud -90,5515442 º.

Figura 2. **Plano de ubicación de la Universidad de San Carlos**

Fuente: Google Maps. http://tinyurl.com/cvdha8z . Consulta: abril de 2015.

1.1.3. Misión

“En su carácter de única universidad estatal le corresponde con exclusividad dirigir, organizar y desarrollar la educación superior del estado y la educación estatal, así como, la difusión de la cultura en todas sus manifestaciones. Promoverá por todos los medios a su alcance, la investigación en todas las esferas del saber humano y cooperará al estudio y solución de los problemas nacionales.”

1.1.4. Visión

“La Universidad de San Carlos de Guatemala es la institución de educación superior estatal, autónoma, con una cultura democrática, con enfoque multi e intercultural, vinculada y comprometida con el desarrollo científico, social y humanista, con una gestión actualizada, dinámica, efectiva y con recursos óptimamente utilizados para alcanzar sus fines y objetivos, formadora de profesionales con principios éticos y excelencia académica.”

1.1.5. Valores

“La universidad, a través de las funciones de investigación, docencia y extensión, crea, cultiva, transmite y difunde el conocimiento científico, tecnológico, histórico, social, humanístico y antropológico en todas las ramas del saber. Evalúa periódicamente los currículos para que se vincule la docencia con la realidad y se desarrolle la sensibilidad social, tomando en cuenta los valores de verdad, libertad, justicia, respeto, tolerancia y solidaridad, estableciendo carreras prioritarias, de acuerdo a las necesidades de desarrollo del país, dentro del contexto regional e internacional.”

1.1.6. Principios

Los principios rectores son la capacidad de autogobierno, la universalidad de ideas, pluralismo ideológico-político, tolerancia, dignidad de la persona y reivindicación social. Sus herramientas son el manejo propio del saber, la producción y adecuación de los conocimientos, el ejercicio de la discusión y del debate intelectual, la no-sujeción a dogmas y la voluntad de brindar bienes y servicios a la sociedad guatemalteca que la sustenta.

1.1.7. Carreras que se imparten

Las carreras que se imparten en la Universidad de San Carlos de Guatemala, están por áreas, las cuales, básicamente están divididas de la siguiente manera:

Área técnica

- Facultad de Agronomía
- Facultad de Arquitectura
- Facultad de Ingeniería
- Facultad de Ciencias Químicas y Farmacia

Área de Ciencias de la Salud

- Facultad de Ciencias Médicas
- Facultad de Odontología
- Facultad de Medicina Veterinaria y Zootecnia
- Escuela de Ciencias Psicológicas
- Escuela de Ciencias y Técnicas de la Actividad Física y el Deporte

Área Social-Humanista

- Facultad de Ciencias Económicas
- Facultad de Ciencias Jurídicas y Sociales
- Escuela de Ciencia Política
- Escuela de Ciencias de la Comunicación
- Escuela de Ciencias Lingüísticas
- Escuela de Formación de Profesores de Enseñanza Media
- Facultad de Humanidades
- Escuela de Historia
- Escuela Superior de Arte
- Escuela de Trabajo Social

1.2. Tecnología

Conocimientos técnicos, que permiten crear bienes o servicios que facilitan la adaptación al ambiente y satisfacer tanto las necesidades esenciales como los deseos de las personas.

1.2.1. Definición

La tecnología es un conjunto de procesos, conocimientos y técnicas, que se utilizan para diseñar y construir objetos para satisfacer muchas de las necesidades humanas.

Figura 3. **La tecnología utilizada para satisfacer necesidades humanas**

Fuente: 2BP Blog de ciencia y tecnología. http://bit.ly/1LDGnEn . Consulta: mayo de 2015.

La tecnología es producto de la ciencia y la ingeniería, aunque muchos de los avances en tecnología sean posteriores a estos dos conceptos anteriores.

Históricamente la tecnología ha sido utilizada para satisfacer muchas de las necesidades humanas (alimento, vestido, vivienda, protección, socialización y comprensión del mundo natural) e incluso para satisfacer algunos placeres corporales y estéticos (cultura, deportes y artes).

En general la tecnología no puede considerarse totalmente beneficiosa ni tampoco lo contrario ya que puede ser utilizada para generar bienestar o bien para destruir, como por ejemplo, los artefactos bélicos que fueron concebidos con fines destructivos, pero están desarrollados con tecnología avanzada.

1.2.2. Tipos de tecnología

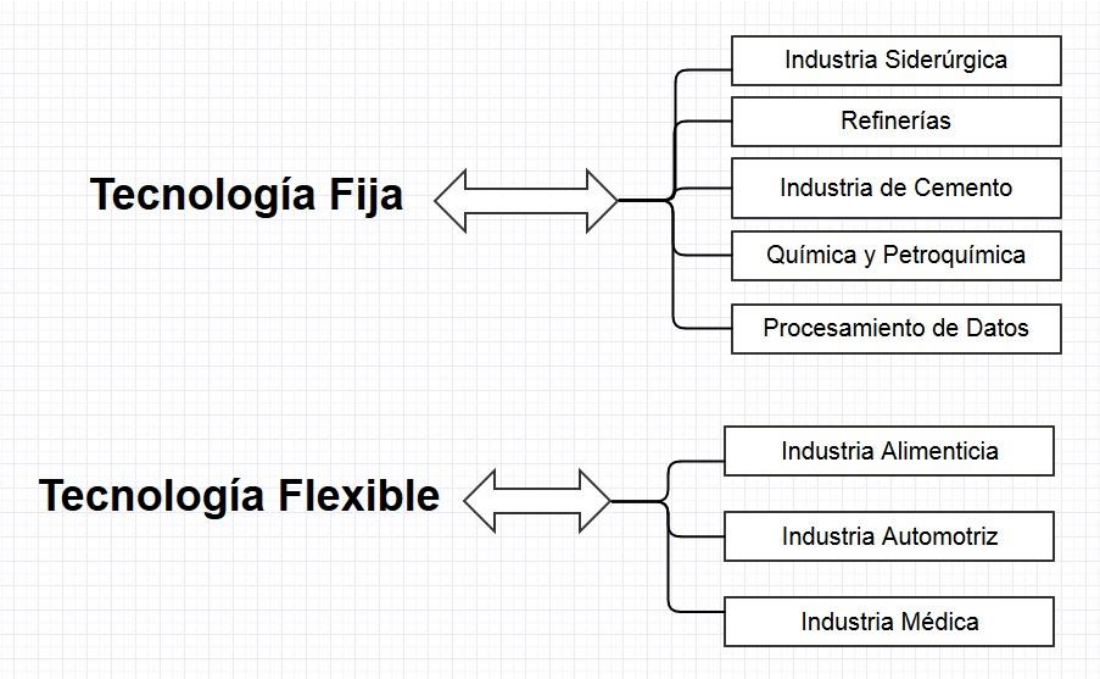
Básicamente existen dos tipos de tecnología según Thompson:

"Tecnología flexible: la flexibilidad de la tecnología se refiere a la amplitud con que las máquinas, el conocimiento técnico y las materias primas pueden ser utilizadas en otros productos o servicios. Dicho de otra manera, es aquella que tiene varias y diferentes formalidades por ejemplo: la industria alimenticia, la automotriz, los medicamentos, etcétera.

Tecnología fija: es aquella que no puede utilizarse en otros productos o servicios. También puede decirse que es aquella que no está cambiando continuamente, por ejemplo: las refinerías de petróleo, la siderúrgica, cemento y petroquímica." [1]

[1] THOMPSON, James D. Organizations in Action: Social Science Bases of Administrative Theory. p. 192.

Figura 4. **Tipos de tecnología según James D. Thompson**



Fuente: elaboración propia.

1.2.3. La tecnología en una institución educativa

Es cada vez más difícil encontrar en estos días, instituciones de cualquier tipo que no tengan implementadas o que estén por implementar tecnologías de información como medio para lograr eficacia y eficiencia en sus operaciones.

Las empresas industriales, generalmente, manejan equipos y maquinaria en sus procesos y estas tienden a usar tecnología en sus programas de capacitación y desarrollo.

Empresas como IBM destinan presupuestos gigantescos a la capacitación y muestran poca resistencia a que su entrenamiento convencional emigre a las computadoras, satélites, buscadores y videoconferencias. Es más probable que las instituciones académicas, por el contrario, sean tecnófobas.

Los profesores y el personal temen a las computadoras y a todas las concepciones erradas asociadas con ellas. La tarea de llevarles tecnología es ardua y los resultados tardan en llegar.

Uno de los problemas mayores a que se enfrentan las instituciones educativas es la resistencia, el llamado analfabetismo tecnológico, que se refiere a tener poco o ningún grado de conocimiento de tecnologías de información. El rol tan importante que juega el educador en esta labor es que, lejos de ser solamente un transmisor de conocimientos teóricos, se transforma en un facilitador del aprendizaje, así como, un dinamizador de la innovación e investigación que se puede realizar en el aula, utilizando tecnologías de información.

1.3. Información

Cuando se habla de informática generalmente se tiende a pensar en equipos sofisticados, grandes computadoras, aplicaciones y nuevos dispositivos, novedosas maneras de elaborar informes, estadísticas, etcétera. Sin embargo, se suele pasar por alto o se tiene en muy poca consideración lo que realmente hace posible la existencia de los anteriores elementos.

Esta base es la información. Y es que la información en la actualidad se ha constituido como un valioso bien que poseen todas las empresas.

Se puede definir exactamente la información como un bien intangible, tanto por poseer un alto valor, no sólo monetario, sino también porque los datos que se manejan en el mundo moderno poseen un alto valor informativo, de ahí que se escuche mucho un refrán que se ha popularizado en la actualidad: la información es poder.

La información es el principal patrimonio de cualquier organización, por lo que su protección y seguridad resulta muy importante, máxime en un momento en el que Internet y las transacciones electrónicas se han establecido como la nueva forma de relacionarse, con ventajas innegables, pero también con los riesgos que ello conlleva.

1.3.1. Importancia

Un bien, no importando de qué tipo se trate, tiene un valioso lugar en las empresas, no sólo porque el poseerlo da ventajas competitivas frente a otras empresas y al mundo informatizado, sino que también constituye un bien que se debe cuidar, como si se tratase de algo tangible como joyas, dinero u otros bienes de alto valor monetario.

Y es que la importancia de la información radica en que el poseerla da ventajas y mantenerla resguardada es un compromiso de la empresa a todos niveles, porque, si la información no se tiene o se deja de tener por cualquier motivo, puede ocasionar pérdidas cuantiosas de dinero.

1.3.2. Costo

El costo podemos definirlo como el gasto en que se incurre para la fabricación de productos o también para prestar un servicio.

La información tiene un implícito valor monetario o en términos administrativos más precisos se le llama costo, debido a que un costo por definición, se refiere a una inversión que retornará a la empresa con una utilidad luego de algún proceso de transformación, su venta directa a los clientes u otras empresas para que puedan procesarla o bien utilizarla para ofrecer algún producto o servicio derivado de los datos que se les ha proporcionado a través de la venta o cesión de información.

1.3.3. Valor

Al referirse a valor, generalmente se piensa en términos que tienen que ver con dinero, aunque esto muchas veces es cierto, no lo es del todo, porque el valor de algún bien o servicio no sólo se puede medir en unidades monetarias, sino que, el valor asociado puede ser medido en otras unidades.

Por ejemplo, si ocurriera algún siniestro o algún accidente en el centro de cómputo de la empresa, eso podría convertirse en graves pérdidas para la empresa no sólo de dinero, sino de tiempo, sueldos pagados, productos o servicios no entregados a tiempo, demoras y también el costo de los equipos dañados, su reparación, la recuperación de la información, así como, su restablecimiento para tener nuevamente el mismo ritmo de trabajo, como hasta antes del problema.

Pero sobre todo, después de un siniestro, una pérdida muy importante puede ser la confianza de los clientes internos como externos y eso deriva en pérdida de credibilidad y confiabilidad de los productos y esto conlleva a pérdidas, no solamente económicas.

1.4. Principios básicos sobre seguridad

La seguridad de la información está ligada con los principios básicos sobre seguridad: confidencialidad, integridad y disponibilidad. Estos principios, están diseñados para contrarrestar los ataques a la seguridad de los sistemas de la institución.

1.4.1. Confidencialidad

Intenta prevenir la revelación no autorizada, intencional o no, del contenido de un mensaje o de información en general. La pérdida de información puede producirse de muchas maneras, por ejemplo, por medio de la publicación intencional de información confidencial de una organización o por medio de mal uso de los derechos de acceso en un sistema. Esto es, exponer de alguna manera, información valiosa que pueda poseer la empresa, como por ejemplo, bases de datos, informes o datos que son de uso exclusivo, que han sido comprados a terceros o bien elaborados para servir a un propósito especial y que debe resguardarse del dominio público.

1.4.2. Integridad

Es la garantía de que la información es exacta y completa, así como, los métodos de su procesamiento. Básicamente se pueden mencionar tres propósitos principales para los cuales la integridad asegura que:

- No se deben realizar modificaciones de datos en un sistema por personal o procesos no autorizados.

- No se deben realizar modificaciones no autorizadas de datos por personal o procesos autorizados.

- Los datos deben ser consistentes, es decir, la información interna es consistente entre sí misma y respecto de la situación real externa.

1.4.3. Disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. También asegura que el acceso a los datos o los recursos de información por personal autorizado, se produce correctamente y a tiempo. Es decir, la disponibilidad garantiza que los sistemas funcionan cuando se les necesita.

1.5. Plan de políticas

Un plan de políticas contempla diferentes fases para la definición de los procedimientos, normas y directrices que encausarán las acciones de los colaboradores de la empresa o institución, tanto internos como externos.

1.5.1. Política

Es un proceso orientado hacia la toma de decisiones y tiene como fin reforzar el compromiso y participación del personal, también legítima el uso de la fuerza coercitiva.

1.5.1.1. Definición

La política es una actividad orientada en forma ideológica a la toma de decisiones de un grupo, para alcanzar ciertos objetivos. También puede definirse como el ejercicio del poder para la resolución de un conflicto de intereses. La utilización del término ganó popularidad en el siglo V a.C., cuando Aristóteles desarrolló su obra titulada Política.

1.5.1.2. Fases para realizar una política

La realización de una política comprende básicamente cuatro fases:

- Desarrollo

  Durante esta fase se crea, revisa y aprueba la política. La creación está conformada por la planificación, investigación, documentación y coordinación de la política. La revisión debe llevarla a cabo un individuo o grupo, previo a la aprobación final de la política. La aprobación de la política es obtener el apoyo de la administración para el desarrollo de la misma.

- Implementación

  En esta fase, se llevan a cabo la comunicación, el cumplimiento y las excepciones de la política. La comunicación es la difusión de la política a los afectados directamente por la misma. El cumplimiento se refiere a la ejecución de política, el trabajo en conjunto con las partes involucradas, asegurando que la misma sea entendida por los involucrados.

Las excepciones se refieren a las situaciones donde la implementación de la política no es posible por diversos factores que deben ser contemplados.

- Mantenimiento

Comprende las etapas de concientización, monitorización, garantía de cumplimiento y mantenimiento de la política. La concientización comprende los esfuerzos para garantizar que las personas están conscientes de la política y buscan facilitar su cumplimiento. La monitorización, es seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política.

La garantía de cumplimiento se refiere a las respuestas de la administración a actos u omisiones que resulten en contravenciones de la política con el fin de prevenir que sigan ocurriendo. El mantenimiento es el proceso que garantiza la vigencia y la integridad de la política.

- Eliminación

Esta fase se refiere al retiro y significa que cuando la política ha cumplido con su finalidad y ya no es necesaria (por cambios de tecnología o nuevas políticas generales de la institución), entonces debe ser retirada, archivarla para futuras referencias y documentar la información sobre la decisión del retiro de la misma.

1.5.2. Plan

Un plan se refiere a un programa o procedimiento para conseguir un determinado objetivo. Es un modelo sistemático que se elabora antes de realizar una acción, con el fin de dirigirla y encausarla. En este sentido, un plan también es un documento, que precisa los detalles necesarios para realizar una obra o proyecto.

1.5.2.1. Definición

El plan de empresa, también denominado plan de negocio, proyecto empresarial, estudio de viabilidad o *business plan* (plan de negocios), es un documento escrito, que identifica, describe y analiza una oportunidad de negocio, examina la viabilidad técnica, económica y financiera de la misma y desarrolla todos los procedimientos y estrategias necesarias para convertir la citada oportunidad de negocio en un plan de empresa concreto.

1.5.2.2. Objetivos de un plan

Los objetivos de un plan deben definirse tanto a nivel interno como externo. Y esto debe hacerse desde las normas y procedimientos establecidos en la institución y respetando los objetivos generales de la misma.

- A nivel interno

    - Comprobar la coherencia del proyecto: la realización del plan de empresa permite alcanzar un conocimiento amplio, profundo y objetivo de la empresa que se pretende poner en marcha y constituye para el emprendedor un valioso instrumento para evaluar la viabilidad de su proyecto y reducir considerablemente el riesgo en la puesta en marcha del mismo.

    - Establecer objetivos y planificar su consecución: no sólo se describen todas las áreas del nuevo negocio, sino también se aprende a fijar objetivos y planificar la manera de alcanzarlos. Por ello, permite al emprendedor medir sus expectativas y sustentar las metas posibles de alcanzar.

    - Evaluar el progreso del proyecto empresarial: cuando el nuevo negocio se encuentra en funcionamiento, el plan de empresa servirá como herramienta interna para valorar la marcha de la nueva empresa y sus desviaciones sobre el escenario previsto.

- A nivel externo

De cara al exterior, el plan de empresa constituye una buena tarjeta de presentación y resulta útil a diversos niveles:

    - Obtener la financiación necesaria para lanzar el proyecto o bien mejorar el que ya se tiene en marcha.

    - Optar a posibles subvenciones de las administraciones públicas.

- Encontrar socios o convencer a estos del mérito del proyecto.

El proyecto debe recoger principalmente un modelo de negocio que demuestre que el emprendedor o el equipo de emprendedores han meditado en profundidad los impulsores clave del éxito o el fracaso para su nueva empresa.

1.5.3. Seguridad de información

Se entienden como las acciones preventivas y correctivas encaminadas a proteger información de una empresa o institución. Este concepto no debe ser confundido con el de seguridad informática, ya que este, sólo trata de la seguridad en medios computacionales y la información no solamente se encuentra en medios digitales.

Figura 5. **La Seguridad de Información**

Fuente: WaysIT Tech Global Solutions. http://bit.ly/1HHK8Yj . Consulta: mayo de 2015.

1.5.3.1. Definición

Tiene como finalidad, la protección de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada de los datos que se administran.

También persigue proteger la confidencialidad, integridad y disponibilidad de la información. Independientemente de la forma, los datos pueden ser: electrónicos, impresos, audio u otros.

Por otra parte, la seguridad de la información contempla la implementación de estrategias que cubran los procesos en donde la información es el activo principal.

Estas estrategias deben tener como punto principal el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dichos activos, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

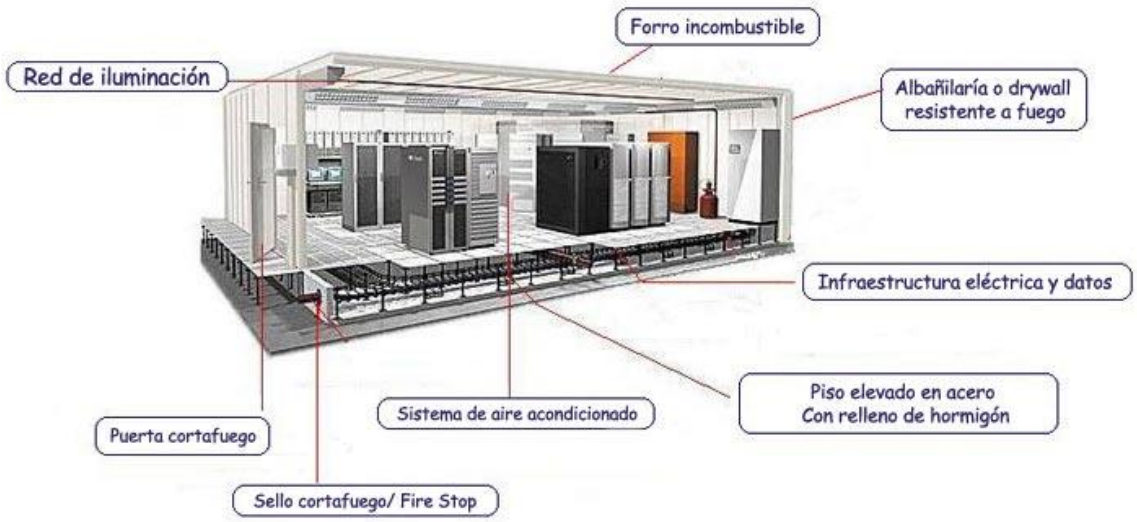
Cabe destacar que la seguridad es un proceso de mejoramiento continuo, por lo tanto, las políticas y controles para proteger información deben revisarse y corregirse, de ser necesario, ante el surgimiento de nuevos retos, esto con el fin de tomar acciones que permitan reducirlos o bien eliminarlos.

1.5.3.2. Seguridad de información ligada a los equipos

Desafortunadamente, la seguridad de información en relación a los equipos es un tema generalmente olvidado con demasiada frecuencia a la hora de hablar de seguridad de información.

En muchas organizaciones se acostumbra tomar medidas para prevenir o detectar accesos no autorizados o denegar servicios, pero rara vez, se previenen las acciones de atacantes que intentan acceder a la sala de servidores o al lugar donde se depositan documentos impresos que son importantes.

Figura 6. **Seguridad en centros de datos**



Fuente: SMH Sistemas de Combate a Incendios. http://bit.ly/1SSlWsp . Consulta: junio de 2015.

Esta situación motiva a que en determinadas ocasiones, un intruso se decline por aprovechar vulnerabilidades físicas en lugar de lógicas, ya que probablemente es más fácil robar un dispositivo físico (memorias, discos, documentos, etcétera) del sistema, que intentar acceder a él mediante fallos en el software.

Se debe ser consciente de que la seguridad física es muy importante como para ignorarla: un ladrón se lleva algún equipo para venderlo, un incendio o un pirata que accede sin problemas a la sala de operaciones puede hacer mucho más daño que un intruso que intenta conectar remotamente con una máquina no autorizada; no importa que se utilicen los más avanzados medios de cifrado para conectar a los servidores, ni que se haya definido una política muy restrictiva a nivel software: si no se tienen en cuenta factores físicos, estos esfuerzos para proteger la información no van a servir de nada.

Además, en el caso de instituciones con requerimientos de seguridad medios, las medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de piratas: como casi todos los atacantes de los equipos de estos entornos son casuales (esto es, no tienen interés específico sobre los equipos, sino sobre cualquier equipo), si notan a través de medidas físicas que la organización está preocupada por la seguridad probablemente abandonarán el ataque para lanzarlo contra otra red menos protegida.

1.5.3.3. Seguridad de información ligada al personal

La seguridad ligada al personal debe ser muy bien planificada. El tratamiento de las medidas de control, aplicadas al recurso humano, requiere mucho tacto y se debe tener en cuenta que cada empleado tiene sus propias determinaciones y condiciones particulares. Sin embargo, es posible crear una planificación de seguridad relacionada al personal, como un conjunto de medidas de control general, que hagan que estas sean efectivas independientemente del sujeto afecto y sin que estas medidas supongan una disminución de los derechos y el confort de los trabajadores. Las principales medidas de control que se suelen recomendar son las siguientes:

Figura 7. **Seguridad de información ligada al personal**

Fuente: Toddle Outsourcing Servicios TI. http://bit.ly/1SSmXk8 . Consulta: junio de 2015.

- Reducir el riesgo del factor humano, por errores, pérdidas, robos o usos indebidos de información.

- Crear conciencia del personal en cuanto a política de seguridad y medidas que deben contemplar para evitar riesgos.

- Minimizar las consecuencias de incidentes provocados por el personal, tomando el error como aprendizaje para la prevención de futuros problemas.

- Estudiar al personal crítico, es decir, a los que deben cubrir tareas críticas de la organización cuya importancia es vital para la empresa.

- Hacer notar en los empleados, la importancia del valor de los activos que están bajo su responsabilidad, no solamente los activos físicos, sino también de la información que en algún momento les es encomendada.

1.6. Mantenimiento

Acciones encaminadas a restaurar o llevar a un estado deseado, cualquier equipo o proceso que lleva a cabo alguna función, es decir, las rutinas necesarias para mantener los activos o instalaciones (planta, equipos, edificio, propiedades inmobiliarias, etcétera) en las condiciones adecuadas para permitir su uso de forma eficiente, tal como está designado.

1.6.1. Definición

Todas las acciones que tienen como objetivo mantener o restaurar un artículo, pueden desarrollarse en diferentes fases y estados del proceso de producción, ya sea en la planificación (mantenimiento preventivo) o sobre la marcha del proceso (mantenimiento correctivo).

1.6.2. Tipos de mantenimiento

En las industrias principalmente, se conocen varios tipos de mantenimiento, pueden ser hasta cinco tipos de mantenimiento los que se pueden encontrar, pero los dos principales tipos de mantenimiento son el preventivo y el correctivo.

Figura 8. **Tipos principales de mantenimiento**

Tipo de mantenimiento	Se efectúa en el:	El costo depende de:
Preventivo	Momento planificado	Lo que se detecte
Correctivo	No se sabe	Del o de los fallo (s) y tiempo consumido por el mismo
Predictivo	Continuamente	Costo de las herramientas usadas

Fuente: GARCÍA GARRIDO, Santiago. Mantenimiento Industrial. http://bit.ly/1HHK8Yj . Consulta: mayo de 2015.

1.6.2.1. Mantenimiento preventivo

Es una actividad programada para inspecciones de funcionamiento como seguridad, ajustes, reparaciones, análisis, limpieza, calibración, que deben realizarse periódicamente, basándose en un plan preestablecido. El fin principal es prever desperfectos en su estado inicial y corregirlos para mantener los equipos o instalaciones en operación a los niveles de eficiencia deseados.

Para los equipos de cómputo se pueden definir algunas de las tareas generales más importantes para realizar mantenimiento preventivo:

- Limpieza general física interna y externa.
- Lubricación y ajuste de partes móviles o mecánicas.
- Ajuste y alineación de unidades de disco, así como desfragmentación y escaneo de errores físicos.
- Limpieza y conservación de los sistemas de ventilación y fuentes de poder.
- Eliminación de software indeseado o que ha sido instalado sin previa autorización del usuario.
- Diagnóstico y medidas de desempeño por medio de software.
- Escaneo con software antivirus y antiespías.

- Instalación y control de actualizaciones de seguridad del sistema operativo.

Figura 9. **Mantenimiento preventivo en software**

Fuente: SOTO, Jesús. Mantenimiento de Software. http://bit.ly/1SSnnqL. Consulta: junio de 2015.

1.6.2.2. Mantenimiento correctivo

Corrección de los desperfectos o fallas de los equipos o procesos, contrario al caso del mantenimiento preventivo que se realiza previendo las fallas. Se puede hablar de dos clases de mantenimiento preventivo:

- Planificado: el cual consiste en la reparación del equipo o proceso cuando se dispone de los repuestos, personal, herramienta y la debida documentación para realizarlo.

- No planificado: es el que regularmente se realiza después de una falla que no se previó y generalmente obliga a detener el proceso o los equipos en cuestión.

Figura 10. **Mantenimiento correctivo en hardware**

Fuente: WebMe, Tecnología avanzada. http://bit.ly/1SSnGSt . Consulta: junio de 2015.

1.6.2.3. Mantenimiento predictivo

El mantenimiento predictivo es una técnica para pronosticar el punto futuro de falla de algún componente de una máquina, de tal forma que dicho componente pueda reemplazarse, con base en un plan determinado, justo antes de que falle. De esta manera, el tiempo de inactividad o tiempo muerto del equipo se minimiza y el tiempo de vida del componente se maximiza.

Además de prever el fallo catastrófico de una pieza o de un sistema completo debido a la falla de alguno o varios de sus componentes, y por lo tanto, el anticiparse a éstas fallas, las técnicas de mantenimiento predictivo ofrecen una ventaja adicional: la compra de repuestos se realiza cuando se necesita y en un tiempo programado, eliminando capital inmovilizado, que muchas veces supone costos de almacenamiento, espacio o simplemente inversión que no supone ninguna ganancia para la empresa o institución.

El mantenimiento predictivo ofrece muchas ventajas, entre las que podemos mencionar:

- Se evitan prácticamente todas las paradas no planificadas por avería.
- Se alargan los intervalos productivos entre paradas para mantenimiento y se minimizan los tiempos de reparación.
- Por lo tanto, se aumenta la disponibilidad de los equipos y los servicios que se prestan.
- Se evitan las pérdidas por paros en el proceso productivo.

- Se amplía la duración de servicio de los componentes, solamente se sustituyen cuando comienzan a dañarse.

- Se reducen los stocks de piezas o equipos para repuesto, ya que el aprovisionamiento de estas piezas también puede programarse.

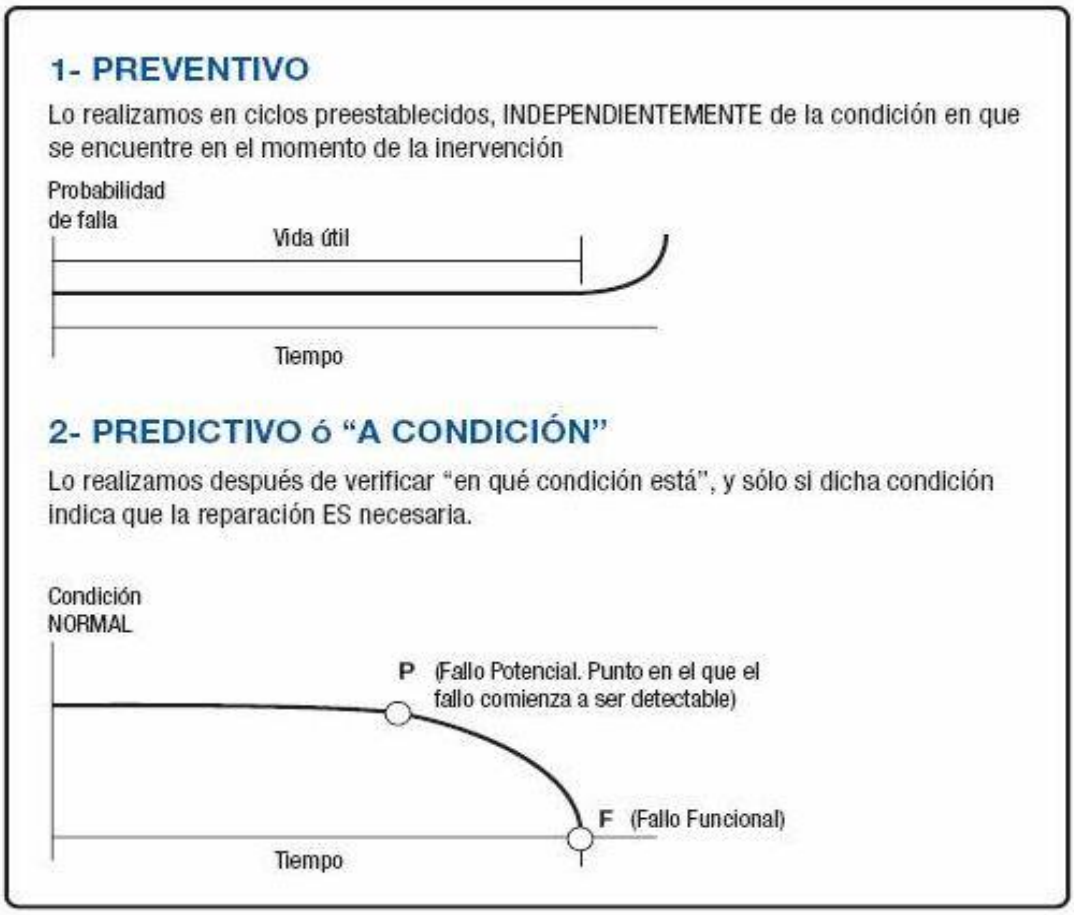
- Se impiden penalizaciones por retrasos y se gana credibilidad por entregas a tiempo.

- Se mejora la calidad de los productos o servicios que se ofrecen a los clientes internos y externos.

- Se evitan averías catastróficas, aumenta la seguridad de la institución, se reducen las primas de seguros.

- En definitiva, se aumenta la fiabilidad de la institución.

Figura 11. **Mantenimiento predictivo en equipo de cómputo**



Fuente: La cultura de la confiabilidad. http://bit.ly/1AHzQI8 . Consulta: junio de 2015.

2. DIAGNÓSTICO, EVALUACIÓN Y ESTUDIO

2.1. El entorno del departamento

Se refiere a los diferentes factores y variables que afectan o mejoran el desempeño de la empresa o dependencia, este se caracteriza porque dichos factores o variables delimitan el marco en el que actúan las empresas y establecen las circunstancias en que estas se van a desenvolver.

Figura 12. **El entorno de una organización**

Fuente: Fundamentos de mercadotecnia. http://bit.ly/1GYfFXi. Consulta: junio de 2015.

2.1.1. Factores ambientales

Los factores ambientales son los que determinan cómo se puede ver afectada o beneficiada una empresa en relación a su situación de competencia, recursos, factores externos que no son controlables, factores internos que pueden ser controlados y todos los elementos que puedan afectar de alguna manera el funcionamiento y los objetivos de la empresa.

2.1.2. Estructura organizativa

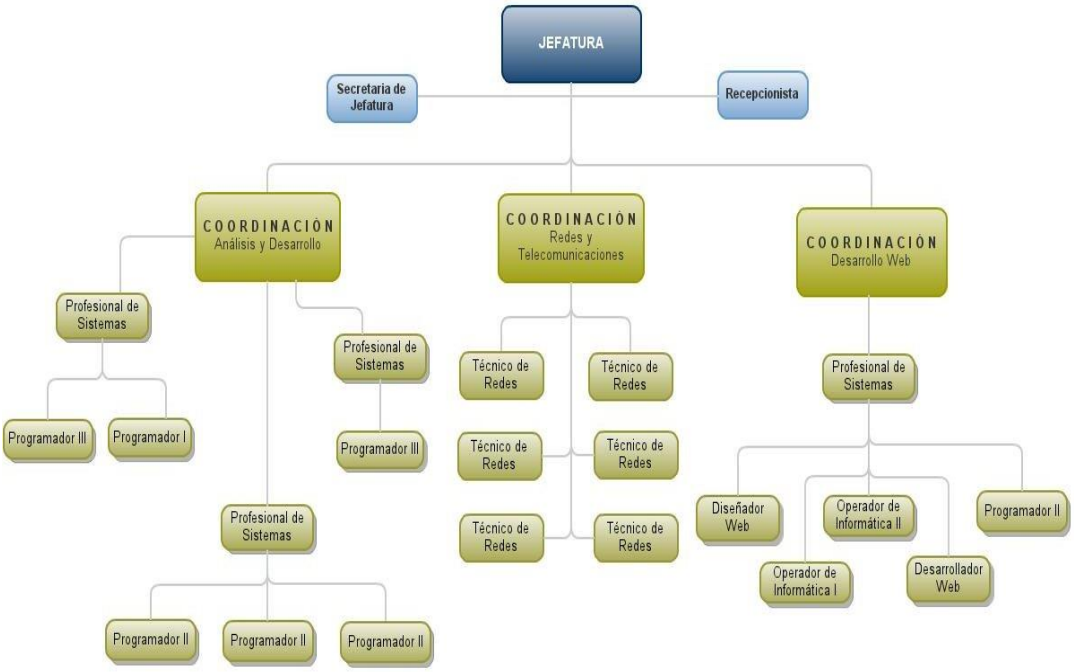
La estructura organizativa del departamento, fundamentalmente se basa en tres áreas o coordinaciones que se constituyen como los mandos medios del departamento y cada una tiene sus tareas específicas asignadas bajo las directrices de trabajo del departamento y en concordancia con los planes de jefatura para realizar su trabajo.

- Grupos de trabajo

  Los grupos de trabajo están actualmente definidos por cada área del departamento, las cuales son tres:

  - Redes y telecomunicaciones
  - Análisis y desarrollo
  - Desarrollo web

Figura 13. **Organigrama del departamento**



Fuente: elaboración propia.

En cada área existe un coordinador, el cual se encarga de distribuir las tareas, organizar al equipo de trabajo y velar por el cumplimiento de las tareas de los empleados, así como, administrar los diferentes equipos e insumos que tienen asignados para llevar a cabo sus funciones respectivas.

- Responsables por área

Cada coordinador de las tres áreas del departamento cumple sus funciones de acuerdo a las políticas de trabajo establecidas por la jefatura del departamento.

Actualmente, las funciones están derivadas del manual de operación del departamento, este manual data de algunos años atrás, el cual no ha sido revisado ni actualizado recientemente.

2.1.2.1. Recursos

Los recursos son todos los elementos con que cuenta el departamento, básicamente se definirán en cuatro grupos: físicos, económicos, humanos y tecnológicos.

- Físicos

Los recursos físicos que tienen relación directa o indirecta para un posible ataque sobre la seguridad del departamento se pueden clasificar en: documentos físicos y hardware.

Los documentos físicos, son un activo importante para toda empresa ya que pueden comprometer datos importantes por ser fácilmente legibles si ocurre algo que los disponga a cualquier persona.

El hardware comprende todos los equipos informáticos: computadoras, memorias, discos duros, discos compactos (CD, DVD), y cualquier otro medio magnético que pueda almacenar información ya que estos se pueden transportar y constituirse como violación a la seguridad de la información del departamento.

Figura 14. **Recursos físicos**

Fuente: CONDORI, José Luis. IT al alcance de tu mano. http://bit.ly/1GYhaES. Consulta: junio de 2015.

- Económicos

Los recursos económicos con que cuenta el departamento están definidos a través del presupuesto anual asignado a la Universidad de San Carlos de Guatemala, regularmente es una cantidad fija que tiene una estructura predefinida para realizar los gastos de funcionamiento del departamento y una parte se destina a usos diversos o imprevistos.

El departamento en cuestión es parte de la Dirección General Financiera de la Universidad de San Carlos de Guatemala, la cual asigna el presupuesto y recursos necesarios para el funcionamiento, sueldos, pago de prestaciones a los empleados, compra de insumos, así como mantenimiento y reparación de equipo de computación, redes, telecomunicaciones y software con sus respectivas licencias.

Figura 15. **Recursos económicos**

Fuente: Runrunes, Presupuestos. http://bit.ly/1IXwrVH. Consulta: junio de 2015.

El propósito principal del departamento es brindar servicios tecnológicos a todas las unidades académicas, centros regionales, facultades, escuelas y demás dependencias de la universidad.

- Humanos

El departamento cuenta con 30 personas que laboran en 3 áreas cada una con un coordinador, los cuales fungen como subjefes y disponen de recursos informáticos prácticamente similares para llevar a cabo las tareas asignadas a cada una de ellas.

Figura 16. **Recursos humanos**

Fuente: CEDENO, Pablo Josué. Apoyo con los recursos humanos. http://bit.ly/1IXwSzf. Consulta: junio de 2015.

Por la naturaleza de los servicios que debe prestar el departamento y en virtud de las demandas de tecnología y servicios especializados en redes y telecomunicaciones, la jefatura del departamento está a cargo de un profesional del área de Ciencias y Sistemas, los mandos medios están a cargo de profesionales en el área de telecomunicaciones y redes, análisis y desarrollo de sistemas, mantenimiento y reparación de hardware y software. En las diferentes áreas del departamento se desempeñan colaboradores especializados en redes y telecomunicaciones, desarrollo web, análisis y desarrollo de sistemas, diseñadores gráficos y maquetadores, los cuales componen las tres áreas del departamento.

- Tecnológicos

Se dispone de aproximadamente 50 puntos de conexión de red, 30 para el personal y 20 puntos más para servidores y puntos de acceso inalámbricos para disponer de una red wifi interna.

De los servidores con que se cuenta, una buena parte de ellos tienen instalado el Sistema Operativo Linux y el resto tienen Windows Server o Windows 2000.

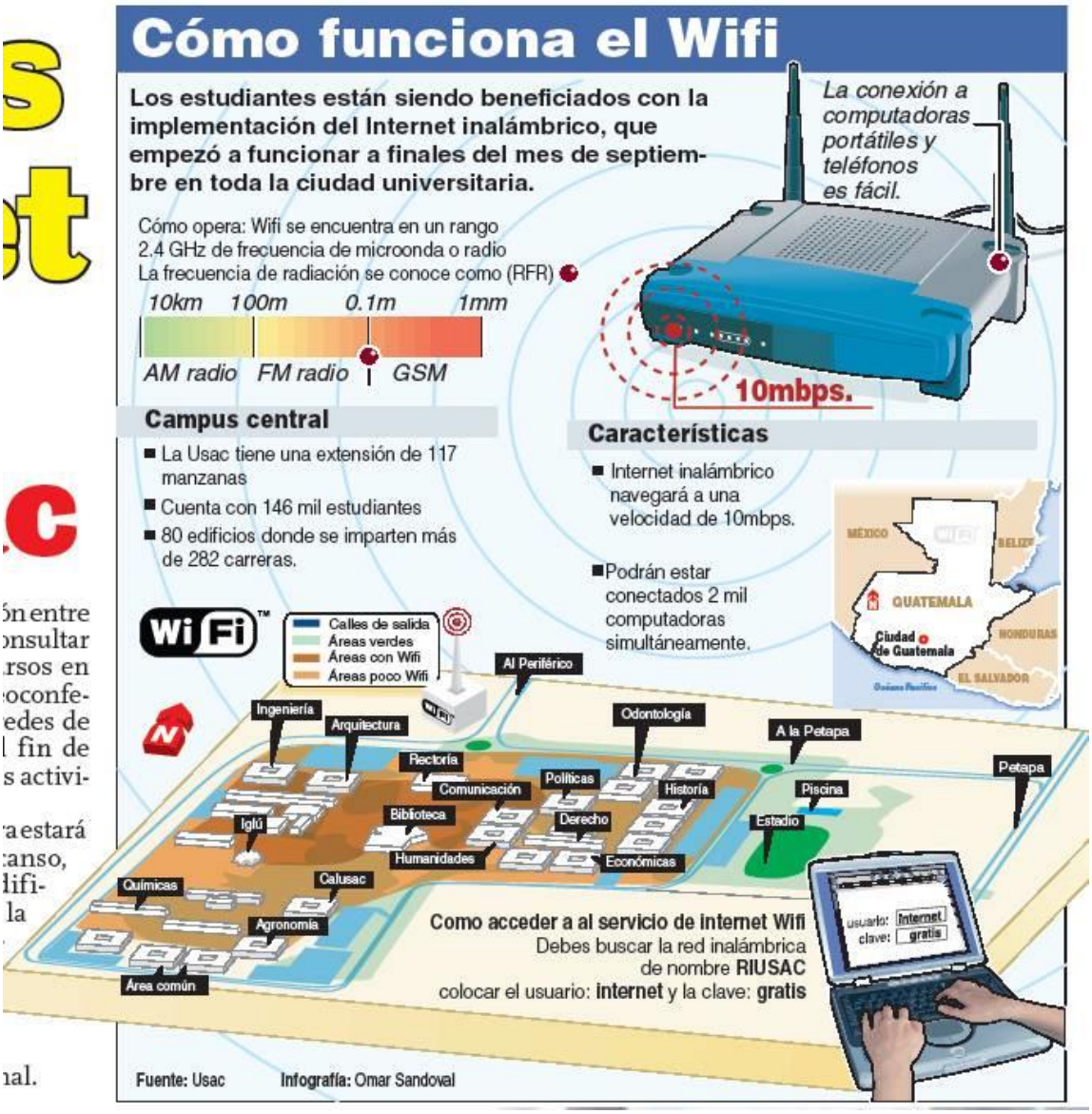
Los recursos de redes y telecomunicaciones se constituyen como los servicios que más cobertura tienen dentro de la universidad, contando entre ellos, el sistema de cableado estructurado, fibra óptica, los enlaces remotos hacia los centros universitarios en el interior de la república.

Figura 17. **Recursos tecnológicos**

Fuente: Red de Empresarios VISA. http://bit.ly/1IXxDZ8. Consulta: junio de 2015.

Los servicios de internet cableados, el servicio gratuito de internet inalámbrico más conocido como wifi, el cual se provee en casi la totalidad del campus universitario especialmente en los exteriores de los edificios principales, así como los servicios de mantenimiento de equipo de computación, certificaciones de equipo e instalaciones así como el desarrollo de software propio de la institución en relación a los sistemas de cobros, caja central, pago de sueldos, presupuesto, auditoría interna, control de correspondencia interna, entre otros.

Figura 18. **Servicio de internet inalámbrico gratuito**



Fuente: SANDOVAL, Omar. Cómo funciona el wifi en la USAC. http://bit.ly/1MjJC4n. Consulta: junio de 2015.

Es importante mencionar que uno de los proyectos de software más importantes y de mayor envergadura dentro de la Universidad de San Carlos de Guatemala es el denominado Sistema Integrado de Información Financiera (SIIF).

El SIIF está compuesto por varios módulos, uno de ellos es el de pagos en línea, en donde se agrupan la mayoría de pagos que los estudiantes realizan, tales como matrícula estudiantil anual, inscripciones, generación de boletas de pago para cursos de vacaciones, exámenes de recuperación, pago de exámenes privados y públicos, pago de alquiler de togas, pago de cursos de idiomas en el Centro de Aprendizaje de Lenguas (Calusac), así como el control de la cuenta corriente de cada estudiante en relación a los años matriculados en cada carrera en que se encuentra inscrito.

Figura 19. **Página web del Sistema Integrado de Información Financiera**

Fuente: elaboración propia.

Por otra parte, se encuentra también el módulo del Sistema Integrado de Compras (SIC) o Gestión Automatizada de Compras, el cual se encarga de llevar el control de todo el proceso, documentación y seguimiento de las compras que realiza la universidad de acuerdo al Decreto 57-92, Ley de Contrataciones del Estado de Guatemala y su Reglamento en conjunto con el Sistema Adquisiciones y Contrataciones del Estado de Guatemala (Guatecompras), para lograr mayor transparencia en dichos procesos.

Además, en el Sistema Integrado de Información Financiera (SIIF) se encuentra el módulo de Nómina o también conocido como Sistema Integrado de Sueldos (SIS).

El SIS es el que se encarga de llevar el control de todas las actividades relacionadas con contratos de trabajo, planillas, pago de sueldos, pago de salarios y prestaciones laborales, cálculo de ISR, declaración jurada de cargos, historial salarial y el control de los datos personales de todos los empleados de la universidad.

Toda la información relacionada a los empleados se maneja desde un sitio web al que pueden acceder todas las unidades académicas, a través de sus encargados de planillas, tesoreros, jefes, profesionales de recursos humanos, profesionales de presupuesto, auditores internos, así como también cada empleado individualmente puede verificar y actualizar la información que se encuentra disponible en el sitio web del SIS.

Figura 20. **Cuenta de empleado en el Sistema Integrado de Salarios**

Fuente: elaboración propia.

Aparte de los proyectos de software también se destaca mencionar los recursos tecnológicos relacionados con el hardware y software disponible que se utiliza para prestar los diversos servicios a la comunidad universitaria.

En relación a los Sistemas Operativos utilizados en el departamento, principalmente se utilizan servidores con Linux y Windows. Estos sistemas operativos son los más populares en el mundo y ambos tienen sus ventajas y desventajas.

Se ha dado a conocer por varios estudios y análisis de expertos en seguridad, que los servidores con Linux, tienden a ser más seguros a largo plazo, aunque sus costos iniciales de instalación suelen ser un poco más altos que los servidores Windows a largo plazo los costos se reducen drásticamente.

Por otra parte, los servidores con sistemas operativos Windows, tienen a incrementar sus costos muy rápidamente de acuerdo a la demanda de programas que necesitemos utilizar debido a las licencias de software que se deben comprar y que resultan tener costos bastante altos en comparación con los sistemas Linux/Unix, los cuales por utilizar la mayoría de programas de código abierto, presentan una mejor opción en cuanto a la relación costo-beneficio.

Figura 21. **Software libre versus software propietario**

	Software libre	**Software propietario**
Ventajas	• Soporte y compatibilidad a largo plazo. • Facilidad de adquisición sin costo. • Libertad de uso y redistribución. • Facilidad de traducir una aplicación en varios idiomas.	• Facilidad de adquisición (puede venir pre instalado o encontrarlo fácilmente en tiendas) • Mayor compatibilidad con el hardware. • Las empresas que los respaldan tienen mas soporte, es decir que son más seguros.
Desventajas	• Inexistencia de garantía por parte del autor. • No hay tanta compatibilidad con Hardware. • Poca estabilidad y flexibilidad en el campo de multimedia y juegos	• El usuario tiene limitadas sus posibilidades de usarlo, modificarlo o redistribuirlo. • A menudo su licencia tiene un costo. • Dependo siempre de la empresa. • Por lo general suelen ser menos seguras

Fuente: 2BP Photobucket, Tipos de Software. http://bit.ly/1dVSMbl. Consulta: junio de 2015.

De acuerdo a Jon C. LeBlanc, en su libro Blanco, asegura que: “La gran cantidad de software de seguridad que no es de Microsoft y los parches de seguridad de los Sistemas Operativos Microsoft atestiguan la debilidad fundamental de los Sistemas Operativos Microsoft en comparación con los sistemas operativos UNIX/Linux.

Esas herramientas de terceros, antivirus y parches de seguridad simplemente no son necesarios en UNIX/Linux. Para ser justos, todos los sistemas operativos pueden ser vulnerables a abusos maliciosos, pero se trata de la gran diferencia para afrontarlos entre UNIX/Linux y los sistemas operativos de Microsoft.”

En relación a los ataques por virus, hackers, etcétera, se tiene mayor confianza en los equipos con Linux, aunque existe un debate en torno al tema, la mayoría de servidores en empresas de alto nivel prefieren a Linux por su estabilidad y menos vulnerabilidad a ataques.

2.2. Análisis de la situación actual

En relación a seguridad de información no existe ninguna política definida que se haya plasmado en algún documento, únicamente hay guías de operación que dan algunas pautas en cuanto a mantener el orden en ciertos aspectos operacionales.

Figura 22. **Análisis del entorno a través de matriz Foda**

Fuente: LÓPEZ, Alfonso. Análisis Dafo. http://bit.ly/1LiGGas. Consulta: junio de 2015.

Uno de los métodos más comunes y sencillos para realizar un análisis de entorno para una empresa, es el conocido como Foda o Dafo que es el acrónimo de Fortalezas, Oportunidades, Debilidades y Amenazas.

La matriz de Foda se utiliza para realizar un análisis que consta de dos partes: una interna y otra externa.

La parte interna tiene que ver con las fortalezas y las debilidades de su negocio, aspectos sobre los cuales usted tiene algún grado de control.

La parte externa se encarga de analizar las oportunidades que ofrecen el mercado y las amenazas que debe enfrentar su negocio en el mercado seleccionado. Aquí se debe desarrollar toda la capacidad y habilidad para aprovechar esas oportunidades y para minimizar o anular las amenazas, circunstancias sobre las cuales se tiene poco o ningún control directo.

2.2.1. Ambiente interno

El ambiente interno puede entenderse básicamente por dos aspectos principales, las fortalezas y las debilidades que tiene la empresa o institución, para este caso se debe analizar qué puntos fuertes y qué puntos débiles tiene el departamento.

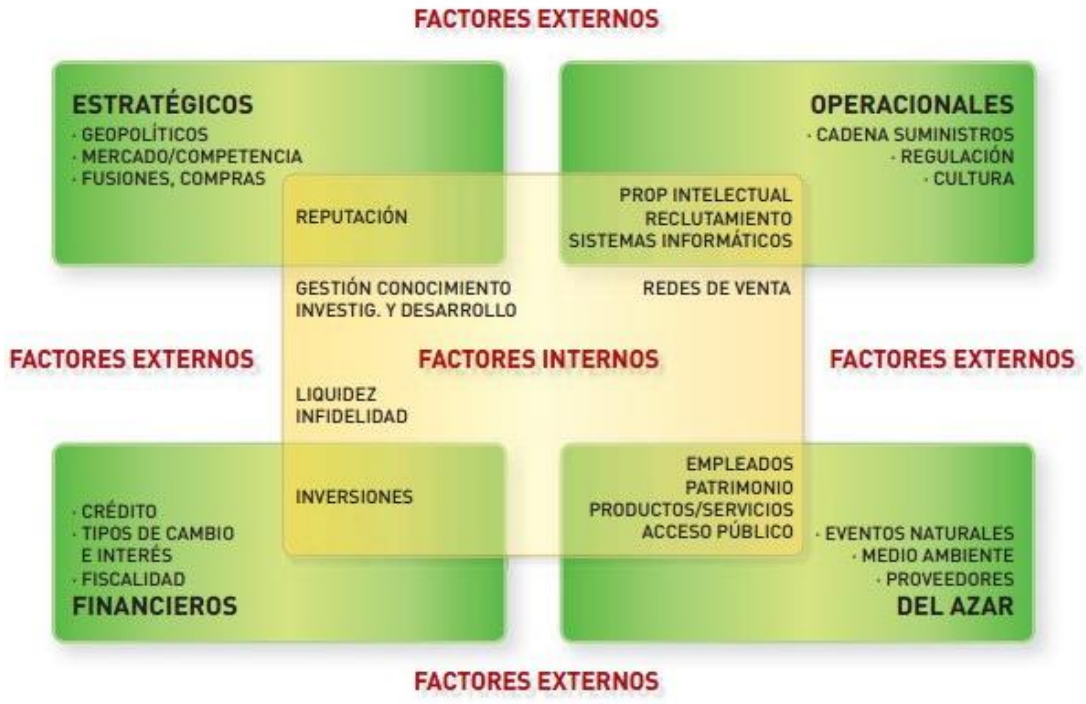
Figura 23. **Análisis interno**

Fuente: Entorno de la empresa. http://bit.ly/1IXvBs4. Consulta: junio de 2015.

En el ambiente interno de departamento se deben tener en cuenta las metas que pretende lograr la organización en un plazo fijado por la planeación. Los objetivos cuantificados, es decir, las metas indicarán los requerimientos futuros de recursos para poder ser alcanzadas.

El departamento debe preparar sus pronósticos económicos. La atención a los clientes internos y externos, el volumen de servicios prestados y los recursos con los cuales se dispone para poder realizar estas tareas. Esos datos son importantes para configurar el monto y la calidad de los recursos humanos que se requerirán para lograr las metas.

Figura 24. **Factores internos y externos para análisis FODA**



Fuente: Seguros Mapfre, Entorno de la Organización. http://bit.ly/1N8bLvs. Consulta: junio de 2015.

Una proyección de necesidades tecnológicas, no solo en su propio campo sino también en administración de procesamiento electrónico de datos, en el plazo de la planeación, es indispensable para tener una idea de los conocimientos y experiencias con que se deberá contar para poder alcanzar las metas propuestas.

El proceso de planeación en toda organización o empresa debe estar allegada a los acontecimientos económicos, sociales y políticos no solo a nivel nacional sino también a nivel internacional debido a que estos cambios pueden ser prejuiciosos para la organización, afectando así su estructura o su factor humano produciendo cambios administrativos o tecnológicos en la misma, modificando las fortalezas y debilidades de la organización, por lo tanto es necesario un sistema para prever dichas evoluciones y anticiparse a las consecuencias de las mismas.

El ambiente interno también se refiere a que la empresa debe estar preparada a enfrentar factores económicos externos. Cabe mencionar que dichos factores afectan directamente a la estructura de la misma relacionando así la economía de la institución con la economía nacional.

2.2.1.1. Fortalezas

Las fortalezas suelen ser los puntos donde la empresa tiene sus mejores cartas, es decir, donde mejor se desempeña o bien donde mejor ha aprendido a desenvolverse. Para este caso, las fortalezas más importantes son:

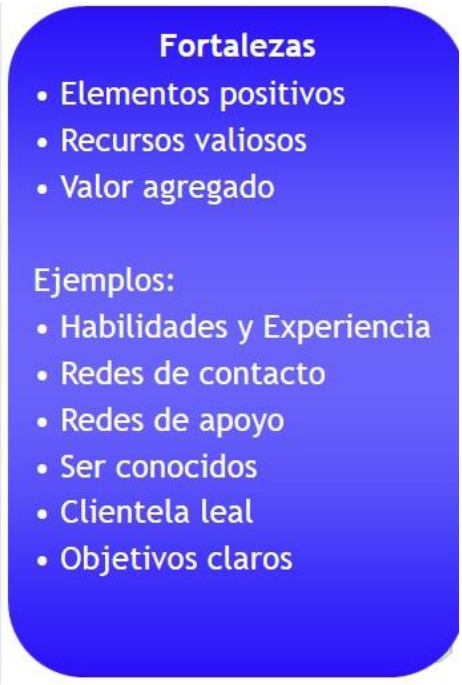
- Los empleados tienen en promedio 5 años de experiencia en sus puestos.

- Se tienen equipos con tecnología al día y eso permite trabajar eficientemente.

- Los mandos medios están involucrados directamente en los proyectos que se desarrollan.

- Se hacen proyecciones anuales con base en los planes y proyectos de la institución y de acuerdo al presupuesto asignado por cada unidad académica, centro universitario, facultad y dependencia.

Figura 25. **Fortalezas en una empresa o institución**



Fuente: DELIZ, Graciana. Análisis Foda, una herramienta de análisis. http://bit.ly/1TDNQIZ. Consulta: junio de 2015.

Todo esto se contempla en el Plan Operativo Anual que contiene un resumen por cada jefatura de lo que se pretende invertir o ejecutar para el próximo año, este plan es elaborado por los coordinadores de área en colaboración con los empleados.

2.2.1.2. Debilidades

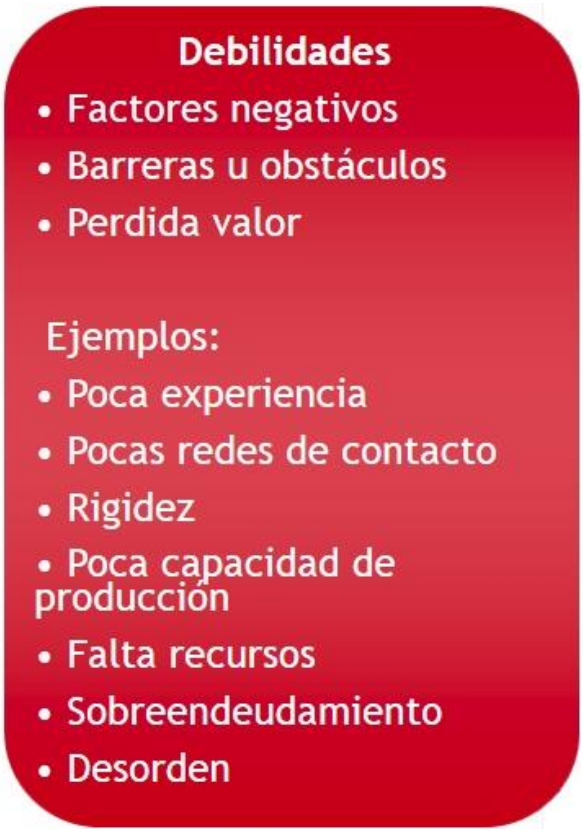
Las debilidades son todos aquellos elementos, recursos, habilidades y actitudes que el departamento tiene y que constituyen barreras para lograr la buena marcha de la institución, a continuación se listan las debilidades más importantes que tiene el departamento:

- Presupuesto limitado y transferido de acuerdo a las políticas de la Dirección General Financiera de la universidad a través del Departamento de Presupuesto.

- No existen documentos en cuanto a funcionamiento y políticas internas en materia de seguridad.

- La seguridad física de los equipos se ha visto comprometida por desastres naturales y no hay políticas de recuperación fiables.

Figura 26. **Debilidades en una empresa o institución**



Fuente: DELIZ, Graciana. Análisis Foda, una herramienta de análisis. http://bit.ly/1TDNQIZ. Consulta: junio de 2015.

2.2.2. Ambiente externo

El ambiente externo representa el entorno que rodea al departamento, en este caso las demás dependencias de la institución, así como, la comunidad universitaria y otros factores externos tales como: factores políticos, legales, sociales, económicos y tecnológicos.

Muchos de los factores externos que afectan a la institución son muy difíciles de controlar debido a que dependen muchas veces de la dinámica de la sociedad, los mercados internacionales, la economía nacional y también los factores ambientales.

2.2.2.1. Oportunidades

Las oportunidades son los factores aprovechables y que pueden traer beneficios al departamento. Se puede decir que son las situaciones externas, positivas, que se generan en el entorno y que al identificarlas, pueden ser de mucha utilidad y beneficio.

Algunas de las oportunidades que se pueden observar en el departamento podemos listarlas a continuación:

- Hay mucha colaboración de instituciones y organismos internacionales que brindan apoyo a la educación, la docencia, la tecnología educativa y en general a las universidades en países que se encuentran en vías de desarrollo.

- El avance de la tecnología siempre se ha considerado como una oportunidad para cualquier institución debido a que al hacer uso de ella, se pueden lograr mayores beneficios que utilizando metodologías tradicionales, es decir, al hacer uso de la tecnología se pueden aprovechar oportunidades de desarrollo.

Figura 27. **Oportunidades en una empresa o institución**

Fuente: DELIZ, Graciana. Análisis Foda, una herramienta de análisis. http://bit.ly/1TDNQIZ. Consulta: junio de 2015.

- Existen muchas herramientas de uso libre y gratuito que de hecho ya se utilizan en el departamento. Entre las herramientas tecnológicas que brindan oportunidades y que se han aprovechado, son las que tienen relación con el software de uso libre.

  Hay algunos ejemplos de herramientas de aprendizaje en línea que se han utilizado para brindar apoyo a la docencia en varias unidades académicas de la universidad a través del departamento.

Por lo tanto, esa es una buena oportunidad de seguir expandiendo ese tipo de servicios que no requieren mayores inversiones monetarias y que refuerzan a las diferentes dependencias educativas de la institución.

- Los colaboradores del departamento son profesionales formados en la misma institución por lo tanto, se constituyen como un grupo alineado con la filosofía y principios de la universidad y que tienen la formación académica necesaria y adecuada para poder implementar soluciones a los problemas y retos que enfrenta el departamento.

2.2.2.2. Amenazas

Cuando algún factor del entorno puede afectar de cualquier manera al departamento, esto se puede considerar como una auténtica amenaza y no se puede pasar por alto, porque podría causar pérdidas de diferente índole.

A continuación podemos listar alguna de las amenazas que pueden afectar al departamento:

- La mala planificación o la planificación unidireccional de parte de la Dirección general financiera puede modificar o entorpecer muchas de las actividades que realiza el departamento.

  En algunas ocasiones se ha dado el caso que se han asignado recursos escasos a renglones de presupuesto que son esenciales para brindar los servicios necesarios a las demás dependencias de la universidad.

- La falta de conocimiento de las políticas internas del departamento pueden dar paso a malas prácticas por parte de los colaboradores en el sentido de no tener los lineamientos necesarios para poder realizar sus tareas de acuerdo a las directrices del departamento.

  Esto sucede muchas veces porque no hay políticas definidas o bien estas no son claras o no han sido expuestas a todo el personal, tampoco existen manuales de operación para empleados con insuficiente información.

Figura 28. **Amenazas en una empresa o institución**

Fuente: DELIZ, Graciana. Análisis Foda, una herramienta de análisis. http://bit.ly/1TDNQIZ. Consulta: junio de 2015.

- Los cambios políticos y económicos en el país siempre son una amenaza para el normal desempeño de toda institución, debido a los cambios en las metas y objetivos de cada dependencia debido a que pueden haber cambios en las jefaturas o bien rotaciones de personal por intereses políticos.

Tabla I. **Matriz Foda**

FORTALEZAS • Los empleados tienen en promedio 5 años de experiencia en sus puestos. • Se tienen equipos con tecnología al día y eso permite trabajar eficientemente. • Los mandos medios están involucrados directamente en los proyectos que se desarrollan. • Se hacen proyecciones anuales con base en los planes y proyectos de la institución y de acuerdo al presupuesto asignado por dependencia. Todo esto se contempla en el Plan Operativo Anual.	**OPORTUNIDADES** • La colaboración de instituciones y organismos internacionales que brindan apoyo a la educación, la docencia, la tecnología educativa y en general a las universidades en países que se encuentran en vías de desarrollo. • La tecnología es una oportunidad para cualquier institución debido a que al hacer uso de ella, se pueden lograr mayores beneficios que utilizando metodologías tradicionales. • Uso de software libre y gratuito. • Los colaboradores del departamento son profesionales formados en la misma institución.
DEBILIDADES • Presupuesto limitado y transferido de acuerdo a las políticas de la Dirección General Financiera de la universidad a través del Departamento de Presupuesto. • No existen documentos en cuanto a funcionamiento y políticas internas en materia de seguridad. • La seguridad física de los equipos se ha visto comprometida por desastres naturales y no hay políticas de recuperación fiables.	**AMENAZAS** • La mala planificación o la planificación unidireccional de parte de la Dirección general financiera puede modificar o entorpecer muchas de las actividades que realiza el departamento. • La falta de conocimiento de las políticas internas del departamento pueden dar paso a malas prácticas por parte de los colaboradores. • Los cambios políticos y económicos en el país siempre son una amenaza para el normal desempeño de toda institución.

Fuente: elaboración propia.

3. PROPUESTA PARA LA IMPLEMENTACIÓN DEL PLAN

3.1. Políticas de seguridad

Una de las premisas más importantes que debe seguirse para proponer o implementar una política de seguridad de información, es la responsabilidad de todos los actores que intervienen en el proceso de administrar la información.

Figura 29. **Aspectos importantes que se deben asegurar**

Fuente: GBC Consulting Group, Gobierno y gestión de servicios de Tic. http://bit.ly/1IXyzNb. Consulta: junio de 2015.

La política de seguridad debe ir enfocada principalmente a tres ejes de acción: personas, procesos y tecnología.

Personas: en este eje se puede hablar de usuarios y el manejo de su entorno de seguridad ya sea en aplicaciones o bien en relación al equipo o dispositivos que manipulan.

Procesos: son los procedimientos o métodos de manipulación de información, o bien el manejo de equipos o dispositivos que contengan información importante y que sea vulnerable.

Tecnología: por ser un departamento de tecnología, este aspecto es importante debido a que se manipulan equipos electrónicos y estos son susceptibles a determinados factores como energía ineficiente, siniestros, robo o copia de información por terceros o bien por el mismo personal interno y pérdidas por defectos en los equipos.

3.1.1. Seguridad física

La seguridad física es la que tiene que ver con todo lo relacionado a los equipos, dispositivos e infraestructura física del departamento, así como, los elementos que inciden en este aspecto. Es importante tener conciencia que por más que la empresa sea la más segura en cuanto a ataques externos, hackers, virus u otras actividades malintencionadas, la seguridad de la misma será prácticamente nula si no se ha previsto cómo evitar o combatir un incendio, inundación, fallas por energía, etcétera.

Uno de los aspectos menos tomados en cuenta a la hora de diseñar un sistema informático es la seguridad física, algunos aspectos se prevén, otros como la detección de un intruso ajeno a la institución que pretende acceder físicamente a cualquier área sensible, no.

Figura 30. **Seguridad física en sistemas informáticos**

Fuente: Varitec de Colombia, Infraestructura y seguridad informática. http://bit.ly/1LqKmnB . Consulta: junio de 2015.

Entonces, la seguridad física según Villalón: es “la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial”[2].

[2] VILLALÓN HUERTA, Antonio. Seguridad en Unix y Redes. Versión 1.2 Digital. http://www.kriptopolis.org. [Consulta: marzo de 2012].

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto, implementados para proteger el hardware y los medios de almacenamiento de datos.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales como: incendios, tormentas e inundaciones
- Amenazas ocasionadas por el hombre
- Disturbios, sabotajes internos y externos deliberados

Ante los desastres naturales lo que se debe tener en cuenta principalmente son estas recomendaciones:

- Cerrar con llave el centro de cómputo. Es una práctica sencilla y fiable para evitar intrusiones.

Figura 31. **Cerrar con llave el centro de cómputo**

Fuente: Direct industry, Seguridad industrial. http://bit.ly/JA2obe. Consulta: junio de 2015.

- Tener extintores debidamente señalizados y ubicados en lugares accesibles, por eventuales incendios.

Figura 32. **Extintores**

Fuente: Prevención laboral y más. http://bit.ly/IkTqh4. Consulta: junio de 2015.

- Instalación de cámaras de seguridad: aunque al inicio requiere de una inversión, es necesario para contar con registros de incidentes en medios digitales de audio y video.

Figura 33. **Cámaras de seguridad**

Fuente: Control electronic security. http://bit.ly/JA1hIH. Consulta: junio de 2015.

- Guardia humana: contar con personal humano para evitar ingresos no autorizados o bien hacer rondas en horas no laborales es una buena práctica para aumentar la seguridad física del departamento. También es importante que de poder contar con guardias, se debe tener control sobre las entradas y salidas de personal tanto propio como externo hacia las áreas donde se encuentran equipos de computación así como dispositivos y otros equipos relacionados con las actividades de la institución para poder brindar mayor seguridad y confianza sobre los activos importantes.

Figura 34. **Guardias de seguridad**

Fuente: PEÑA TABILO, Rocío Belén. Guardia del recinto. http://bit.ly/JA3jIN. Consulta: junio de 2015.

- Control permanente del sistema eléctrico, de ventilación y aire acondicionado, los sistemas de aguas pluviales, sistema de agua potable y también las aguas residuales, las cuales pueden ser un riesgo potencial para las áreas don se encuentran equipos de computación que puedan verse comprometidos físicamente debido a inundaciones por aguas propias o bien pluviales, así como también por descargas eléctricas o incendios provocadas por cortocircuitos o instalaciones defectuosas.

Figura 35. **Inspección de sistemas**

Fuente: Temar ingeniería, mantenimientos. http://bit.ly/Ibt569. Consulta: junio de 2015.

- Inspeccionar las caídas de agua pluvial que puedan afectar áreas importantes en caso de inundaciones.

Figura 36. **Inspección del sistema de aguas pluviales**

Fuente: Instalaciones y aires de Argentina. http://bit.ly/IBB4bJ. Consulta: junio de 2015.

- Se debe tener especial cuidado en el manejo de materiales inflamables en áreas delicadas. Se debe tener un área dedicada al almacenamiento y control de materiales inflamables, corrosivos o que puedan representar u riesgo para la seguridad tanto de los equipos como del personal de la institución, por lo tanto, deben existir controles documentados sobre el manejo y traslado de materiales peligrosos dentro de las áreas del departamento.

Figura 37. **Cuidado en el manejo de materiales inflamables**

Fuente: Carteling, seguridad industrial. http://bit.ly/I1meY6. Consulta: junio de 2015.

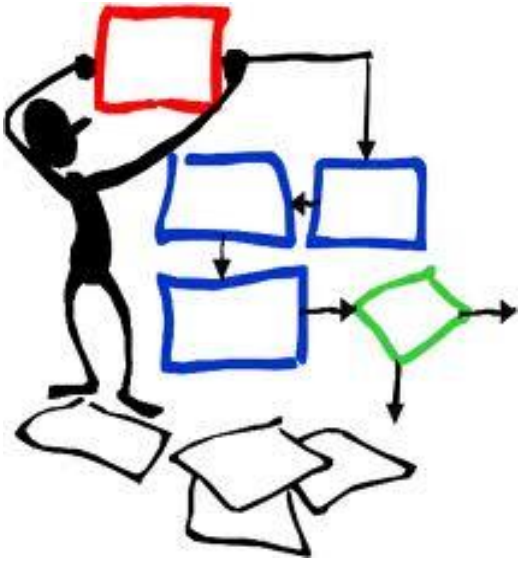
- De ser posible, el cuarto principal del centro de cómputo debe tener un sistema contra incendios en caso de problemas eléctricos o de otra índole. Esto con el fin de tener asegurado en la medida de lo posible todos los equipos principales del departamento, cubiertos para cualquier siniestro relacionado con incendios.

Figura 38. **Sistema contra incendios**

Fuente: Energy Petrol, Kidde fire systems. http://bit.ly/IBBKO2. Consulta: junio de 2015.

- Deben existir procedimientos claros para rescate de equipos en la medida de lo posible. Existen procedimientos para el manejo de dispositivos en caso de haber sido expuestos a daños físicos, esto con el propósito de intentar una recuperación de la información contenida en ellos, con el fin de poder trasladar esa información a otro dispositivo donde la información pueda ser nuevamente utilizada para los procesos productivos del departamento.

Figura 39. **Procedimientos claros y disponibles**



Fuente: OLATE, Claudia. Procedimientos. http://bit.ly/IbslOm. Consulta: junio de 2015.

3.1.2. Seguridad de la red

La planificación de la seguridad de la red es de suma importancia, pues de ello depende mucho, el buen funcionamiento de la misma y esto evita trabajo posterior, pérdida de datos y posibles daños físicos y lógicos.

Muchas veces, el tema de seguridad de la red se considera fuera de tiempo lo cual trae como consecuencia reproceso, gastos innecesarios y posibles pérdidas de información.

Figura 40. **Riesgos de seguridad en una red**

Fuente: Académica, Comunidad digital de conocimiento. http://bit.ly/1LqMziP. Consulta: junio de 2015.

Algunos puntos que se deben tomar en cuenta son:

- Accesos no autorizados
- Daño intencionado y no intencionado
- Uso indebido de información (robo de información)
- Utilización o instalación de aplicaciones que no tienen que ver con el trabajo.

El nivel de seguridad de la red dependerá de su tamaño y del volumen de información que maneje. Por ejemplo, una institución bancaria deberá tener un nivel muy alto de seguridad por las transacciones que maneja, una red pequeña o doméstica no tendrá la misma importancia, sólo se orientará a los accesos de las personas que la utilizan y a ciertos puntos de las computadoras que la forman.

Las políticas referentes a usuarios y contraseñas, los métodos de acceso a los servidores y a los sistemas también deben tenerse muy en cuenta. Se tiene que definir la complejidad que deben tener las contraseñas y su validación dentro de la red, el tiempo de uso de los equipos, áreas de acceso por usuario, horarios para realizar determinadas tareas, control de accesos remotos a través de redes privadas virtuales, etcétera.

3.1.3. Seguridad de usuarios

Por lo general, los esfuerzos de aseguramiento de los equipos y datos, suelen ser muy considerados, sin embargo, la seguridad a nivel de los usuarios, se le suele dar menor importancia o simplemente es pasada por alto.

En estos casos, se habla del enemigo que se tiene dentro de la organización, bien sea por la mala intención de sus actos, o por negligencia en el tratamiento de los activos de la información.

Todas las medidas de control, orientadas al personal, requieren mucho tacto y también tener en cuenta que los empleados tienen sus propias condiciones y determinaciones. Aun así, es posible planificar la seguridad a nivel del personal, como un conjunto de medidas, que sean efectivas, sin importar el sujeto y sin que estas supongan una violación a los derechos y la comodidad de los trabajadores.

Según la Norma ISO 17799 sobre seguridad ligada al personal, son cuatro los aspectos más importantes que deben tomarse en cuenta en relación al tema del personal en la institución o empresa:

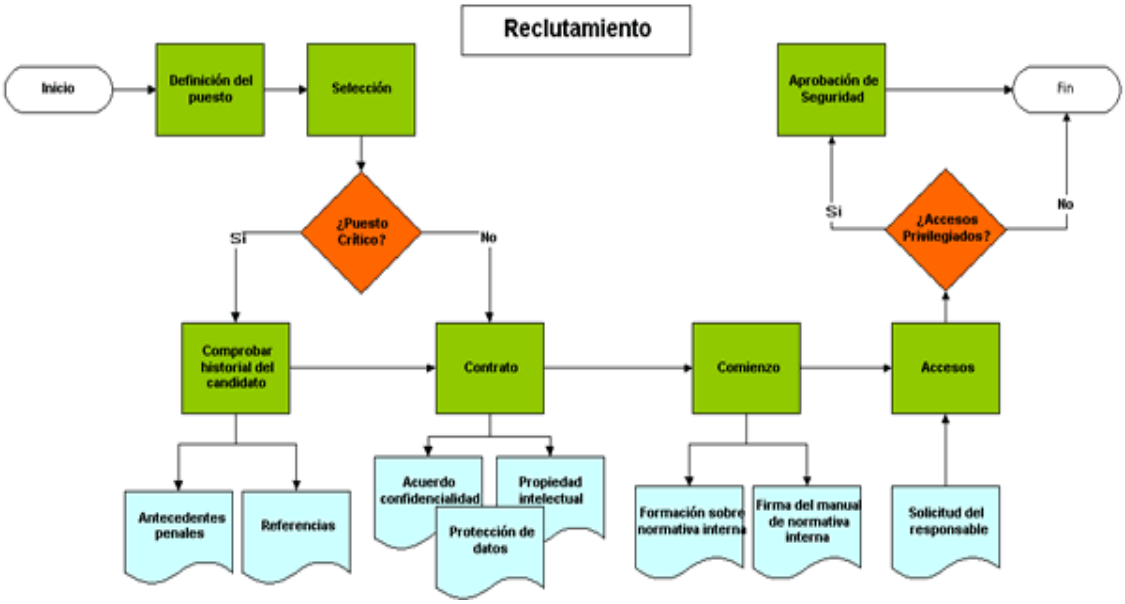
- Reducción del riesgo por factores humanos, debido a errores, pérdidas, robos o usos indebidos de la información. Acuerdos de confidencialidad, selección cuidadosa del personal y tomar en cuenta la seguridad dentro de las responsabilidades desde la contratación, son buenas prácticas aconsejables en este punto.

- Concientizar al personal sobre la política de seguridad y medidas que deben respetar para evitar riesgos innecesarios.

- Minimizar las consecuencias de los incidentes provocados por el personal, tomando el error como aprendizaje para prevenir futuros incidentes. Cuando sea comprobada la mala intención en el personal, es importante que la empresa recurra a procesos disciplinarios y acciones legales sin contemplación.

- Estudio del personal crítico, es decir, del personal que debe cubrir las tareas críticas de la organización cuya importancia es vital para la empresa.

Figura 41. **Diagrama de proceso para seleccionar personal**



Fuente: Rrhh Magazine, Actualidad en recursos humanos. http://bit.ly/1LqM7Ry. Consulta: junio de 2015.

3.1.4. Seguridad de datos

Los verdaderos peligros para la organización en relación a la seguridad de datos son: el espionaje industrial, los ladrones de información, empleados descuidados y las interrupciones de servicios. También se deben tener en cuenta los ataques informales:

- Los irresponsables (un papel con la contraseña escrita)
- Amenazas, sobornos o extorsiones
- Traidores (por ejemplo, empleados resentidos)

- Los no interesados

- Acceso en áreas sensibles

- Ingeniería social, por ejemplo llamando por teléfono a una secretaria

Se necesita una estrategia de seguridad para evitar fugas de información y fallas en los sistemas. Los ataques y vulnerabilidades presentan un factor de riesgo y por lo tanto, pérdida de dinero y confiabilidad por parte de los clientes u otras dependencias de la institución.

La Norma ISO 27001, incluye el ciclo de Deming, el cual trata de cuatro funciones principales para la gestión de un proceso de mejora continua y por la naturaleza del proceso de gestión de la seguridad de información, esto es un apoyo importante para poder definir las tareas de planificar, hacer, verificar y actuar. Estas cuatro tareas serán la base del proceso de mejora continua de la protección de datos en el departamento.

Figura 42. **El ciclo de Deming en ISO 27001**

Fuente: Universidad nacional de Colombia, Planear, hacer, verificar y actuar. http://bit.ly/1fp9VLs. Consulta: junio de 2015.

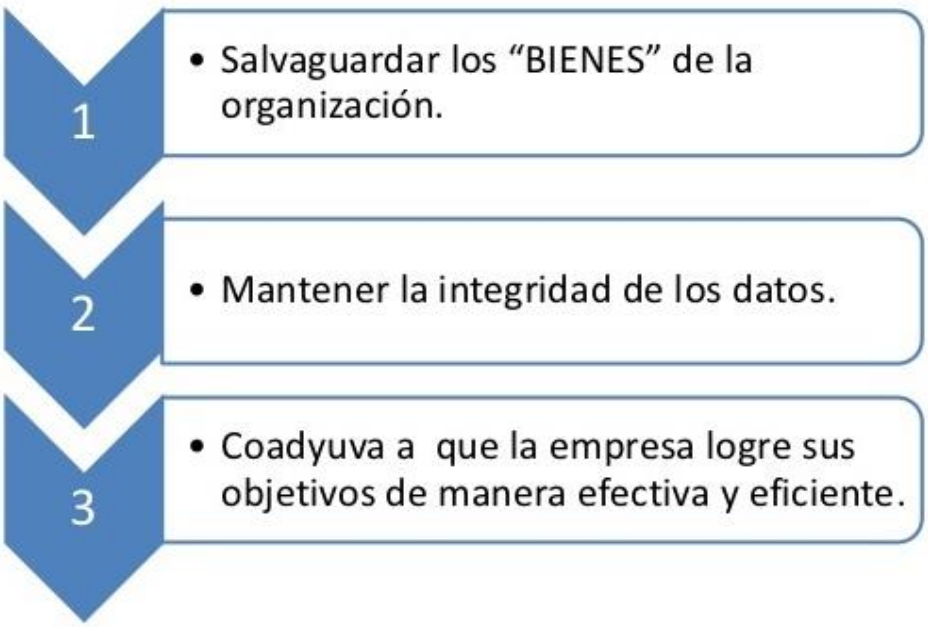
3.1.5. Auditoría de seguridad

Comprende el análisis y el manejo de sistemas, el cual es ejecutado regularmente por ingenieros o técnicos en computación para identificar y describir las vulnerabilidades que pueden suscitarse en una revisión de las estaciones de trabajo, las redes de comunicaciones y los servidores.

Las auditorías de seguridad de información, nos brindan un informe de cómo están nuestros sistemas a nivel de seguridad informática.

El informe final que elaboran los auditores de seguridad de información, indicará las brechas de seguridad encontradas, las medidas y defensas que se deberían aplicar para minimizar los riesgos a los que el departamento pueda estar expuesto. Todo ello debe estar debidamente documentado y debe seguir los lineamientos de las políticas de seguridad de información a que está sujeto el departamento.

Figura 43. **Propósitos de las auditorías de seguridad informática**



Fuente: GIORGI, Alejandro. Auditoría de sistemas. http://bit.ly/1fpc4XD. Consulta: junio de 2015.

3.2. Aspectos organizativos para la seguridad

La seguridad de la organización debe estar coordinada desde los grupos de trabajo, en este caso desde los mandos medios de las diferentes áreas con base a las directrices de la jefatura.

3.2.1. Grupos de trabajo

Los grupos de trabajo tienen como objetivo primordial, recopilar información, analizarla y proponer políticas de privacidad y seguridad de información (datos personales, autenticación, certificados electrónicos, criptografía y seguridad de la información), dirigidas a mantener lo estipulado en las políticas de seguridad de información propias de la dependencia y facilitar los intercambios electrónicos con seguridad y garantías.

3.2.2. Responsables por área

Los responsables por área serán los coordinadores, quienes delegarán funciones de acuerdo al nivel de seguridad de cada colaborador para que cada rol dentro del esquema de seguridad tenga sus propias atribuciones y responsabilidades.

3.2.3. Asignación de responsabilidades por equipo

A cada colaborador en las diferentes áreas se le delegarán responsabilidades de acuerdo a la naturaleza de su puesto y las tareas que desempeña, así como, tomar en cuenta los accesos físicos y electrónicos que posee, para hacer evaluaciones periódicas y determinar si tiene permisos que no le corresponden.

Una técnica muy utilizada para asignar responsabilidad para los colaboradores, se conoce como matriz de asignación de responsabilidades (RAM) por sus siglas en inglés. Esta matriz básicamente permite relacionar actividades con recursos (individuos o equipos de trabajo).

Con esta matriz de asignación de responsabilidades se logra asegurar que cada una de las actividades y cada uno de los proyectos o tareas estén asignados a un individuo o equipo de trabajo.

Tabla II. **Matriz de asignación de responsabilidades**

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES						
Actividad		Roles / Responsabilidades				
Id Actividad	Actividad	Juan	Luis	Margarita	.....	Pedro
Id1	Investigación	X	X			
Id2	Planificación		X	X		
Id3	Desarrollo		X			X
Id4	Seguimiento	X				X
Id5	Mejora continua	X		X		

Fuente: elaboración propia.

3.3. Clasificación y control de equipos

Los equipos de cómputo deben estar debidamente identificados, clasificados y localizados, así como, tener un fácil acceso. Deben estar ubicados de tal manera que puedan aislarse de amenazas tanto físicas como electrónicas.

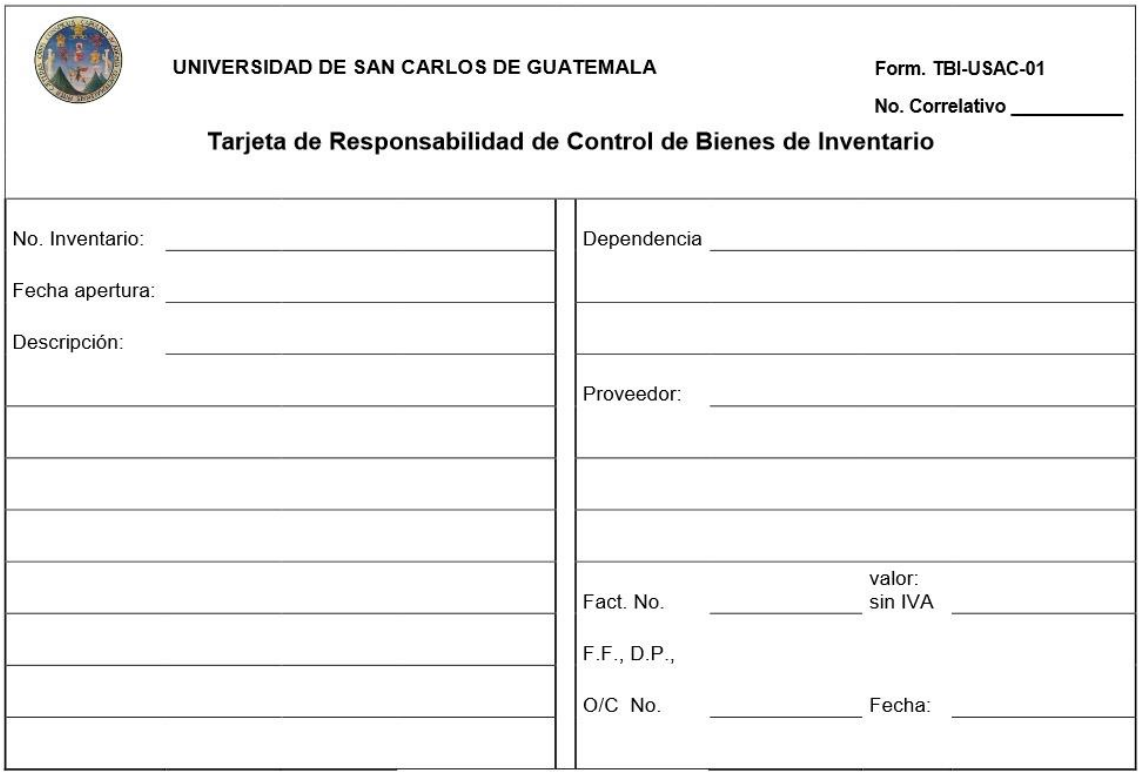
3.3.1. Clasificación de equipos

Todos los equipos deben estar bien clasificados, debido principalmente a su localización y a la persona responsable de los mismos. También puede tomarse como medida, un mapa para ubicar los equipos principales sin necesidad de hacer visitas personales.

En el caso particular de este departamento, ya existe dentro de la Universidad de San Carlos un control interno generalizado para clasificar y poder localizar equipos. El departamento de contabilidad, es el encargado de llevar esos controles, a través de las tarjetas de responsabilidad, las cuales detallan para cada empleado, cuales son los equipos, materiales y herramientas que están bajo su responsabilidad y su respectiva clasificación.

Cada empleado al momento de iniciar relación laboral, se le hace entrega de su respectivo equipo de trabajo, ya sean equipos de cómputo, materiales, herramientas y demás enseres que le puedan ayudar a desempeñarse de mejor manera en su cargo, los cuales serán consignados en la tarjeta de responsabilidad, la cual deberá firmar el empleado para hacerse responsable.

Figura 44. **Tarjeta de responsabilidad para control de bienes**



UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Form. TBI-USAC-01

No. Correlativo _____

Tarjeta de Responsabilidad de Control de Bienes de Inventario

No. Inventario: _____	Dependencia _____
Fecha apertura: _____	
Descripción: _____	
	Proveedor: _____
	Fact. No. _____ valor: sin IVA _____
	F.F., D.P.,
	O/C No. _____ Fecha: _____

Fuente: Dirección de asuntos jurídicos USAC, opinión sobre tarjetas de responsabilidad. http://bit.ly/1GJa6ud. Consulta: junio de 2015.

3.3.2. Localización de equipos

Es muy importante realizar un estudio de la localización, ya que esto permitirá determinar un lugar más adecuado, donde factores como los naturales, de servicios y de seguridad sean los más favorables. Pero si en la organización ya se tiene un lugar definido y no hay otra alternativa, lo único que se puede realizar son los arreglos necesarios para la instalación.

Se debe resaltar que las condiciones físicas del lugar donde se debe ubicar un equipo de computación importante como servidores de datos o aplicaciones, han de ser mucho más rigurosas que las del lugar donde se debe ubicar una computadora personal. También, hay que considerar que una computadora personal puede ser tan importante para una empresa pequeña como un servidor lo es para una empresa grande.

La preparación y adecuación del lugar tiene como finalidad proporcionar los servicios y accesorios necesarios para el buen funcionamiento y lograr la máxima eficiencia operativa.

No sólo se debe tomar en cuenta la ubicación del centro de cómputo, sino también la ubicación individual de cada equipo a ser instalado, porque si se toma en cuenta que desde un extremo del centro de cómputo se debe instalar cierta cantidad de cables y si es posible reubicar ese equipo para un lugar más cercano a los puntos de acceso para la red, la institución está ahorrando buena cantidad de cableado solamente por haber seleccionado una mejor área para la distribución de cableado estructurado, además este ejemplo también desemboca en una menor cantidad de equipo dentro del centro de cómputo, lo cual trae mayor orden y seguridad.

Algunas de las consideraciones más importantes a la hora de planear la instalación, el traslado o la remodelación de un centro de cómputo, son las siguientes:

- Espacio físico: analizar la distribución física tomando en cuenta los suministros de energía, servicios de agua, aire acondicionado, sistema de seguridad, accesos para el personal y almacenamiento.

- Movilidad y distribución: características de las instalaciones, alto, ancho, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil, etc.

- Paredes y techo: las paredes irán con pintura plástica, no-inflamable y lavable para poder limpiarlas fácilmente y evitar la erosión.

- El techo real deberá pintarse, así como las placas del techo falso y los amarres, la altura libre entre el piso falso y el techo falso debe tener una altura considerable de acuerdo a estándares de construcción seguros, para permitir la movilidad del aire.

- Piso y pisos falsos: se debe tener en cuenta la resistencia para soportar el peso del equipo y del personal, es mejor usar placas metálicas o de madera prensada para el piso falso con soportes y amarres de aluminio, con sellos herméticos y nivelado topográfico realizado por profesionales. También se debe considerar la posibilidad de realizar cambios en la ubicación de los equipos, además de cubrir los cables de comunicación entre la unidad central de proceso, los dispositivos, las cajas de conexiones y cables de alimentación eléctrica.

  La altura recomendable será de 18 a 30 cm. si el área del centro de procesamiento de datos es de 100 metros cuadrados o menos, con objeto de que el aire acondicionado pueda fluir adecuadamente.

- Puertas de acceso: tener en cuenta las dimensiones máximas de los equipos si hay que atravesar puertas y ventanas de otras dependencias. Las puertas deben ser de doble hoja y con una anchura total que supere fácilmente el tamaño de los equipos más grandes que pueda ser necesario pasar por dichas puertas. Crear rutas de salida en caso de emergencia.

Figura 45. **Ubicación para el centro de cómputo**

Fuente: XperTic de México, Datacenters. http://bit.ly/1KkZ4xx. Consulta: junio de 2015.

3.3.3. Responsables de los equipos

Los empleados deben tener asignados a través de algún documento de responsabilidad, los equipos que están a su cargo para determinar en cualquier momento a qué empleado se le han asignado equipos, herramientas y materiales, los cuales estarán bajo su responsabilidad.

Regularmente, estos documentos se conocen como tarjetas de responsabilidad y es algún delegado de contabilidad o inventarios quien se encarga de consignar dicha información para que esté disponible y sea fácil de verificar.

3.4. Control de accesos

El acceso a los diferentes entornos de la organización que manejen información importante no solamente se debe cuidar desde y hacia la red o dispositivos electrónicos, también debe hacerse un estudio de los accesos físicos, es decir, si algún intruso, ya sea externo o de la misma organización puede llegar sin mayor dificultad hacia alguno de los entornos que manejan información importante para la organización.

Figura 46. **Control de accesos internos**

Fuente: Seguridad física. http://bit.ly/1H35BvP. Consulta: junio de 2015.

3.4.1. Accesos internos

Los accesos internos pueden ser desde la red interna, por medio de dispositivos portátiles o bien simplemente accediendo directamente hacia alguno de los ambientes de la organización donde se maneja o almacena información. Se debe tener especial cuidado a los accesos dentro de los ambientes ya que puede significar intrusiones muy graves en áreas delicadas aunque estas sean accidentales.

3.4.1.1. Equipos

Los equipos deben estar asegurados desde la perspectiva de mantener el escritorio limpio, lo cual significa, mantener el equipo asegurado del robo de información, protegido por contraseña y no dejarlos escritos a la vista, así como, no utilizar palabras obvias como su nombre.

Un sistema de gestión de seguridad de información, exige que para todos los lugares de trabajo, especialmente los que tienen que ver con asuntos tecnológicos, se debe adoptar una política de escritorio limpio, lo cual significa evitar riesgos de seguridad por simples descuidos del usuario, a través de poner en riesgo los activos de la institución.

Algunas de las recomendaciones importantes para este tipo de política son:

- No dejar la computadora desbloqueada si va a salir, aunque sea por unos pocos minutos.

- No dejar documentos de ninguna clase con contraseñas o pistas para poder ingresar a cualquiera de los sistemas que están bajo su responsabilidad.

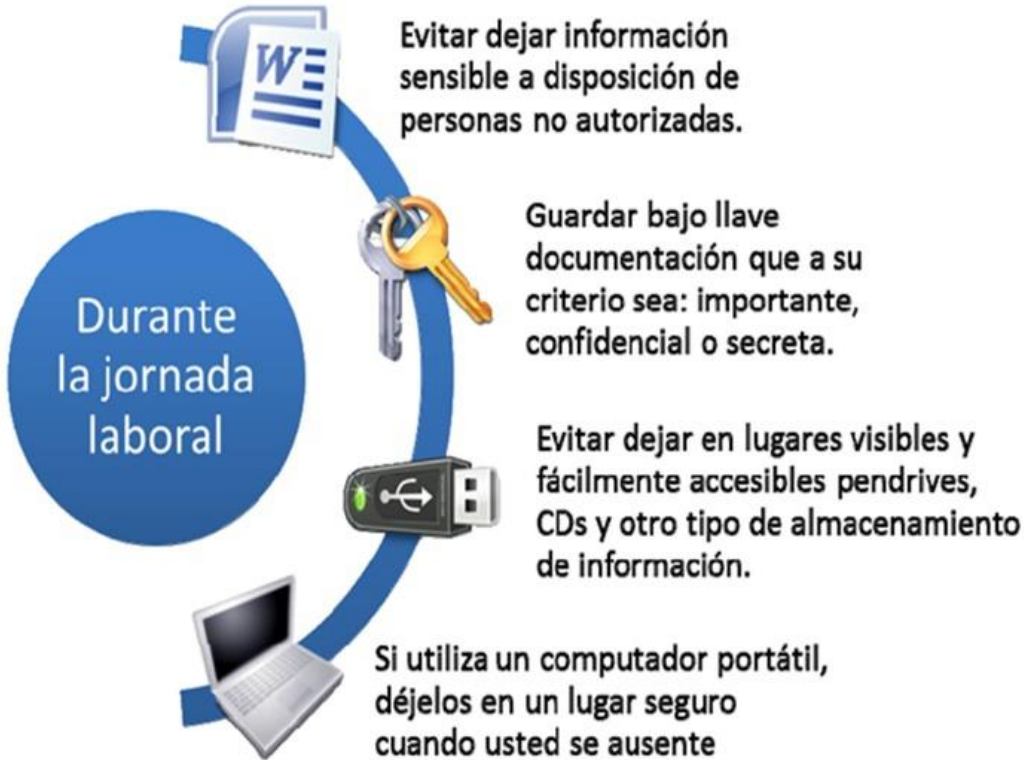
- No dejar olvidados documentos en impresoras, escáneres o fotocopiadoras que puedan contener información sensible de la institución, información propia o información de terceros.

- No dejar sobre el escritorio computadoras portátiles, teléfonos celulares, tabletas o agendas electrónicas y ninguna clase de aparatos electrónicos que puedan contener información personal o de la institución.

- No olvidar llaves físicas, ni tarjetas de acceso a los diferentes ambientes del departamento.

- Tener control de dispositivos y equipos de almacenamiento de información tales como memorias USB, discos duros externos, CD, DVD o cualquier otro medio que pueda contener información sensible.

Figura 47. **Política de escritorio limpio**



Fuente: Intendencia región de Atacama, Chile. Política de escritorio limpio. http://bit.ly/1H38VY2. Consulta: junio de 2015.

3.4.1.2. Aplicaciones

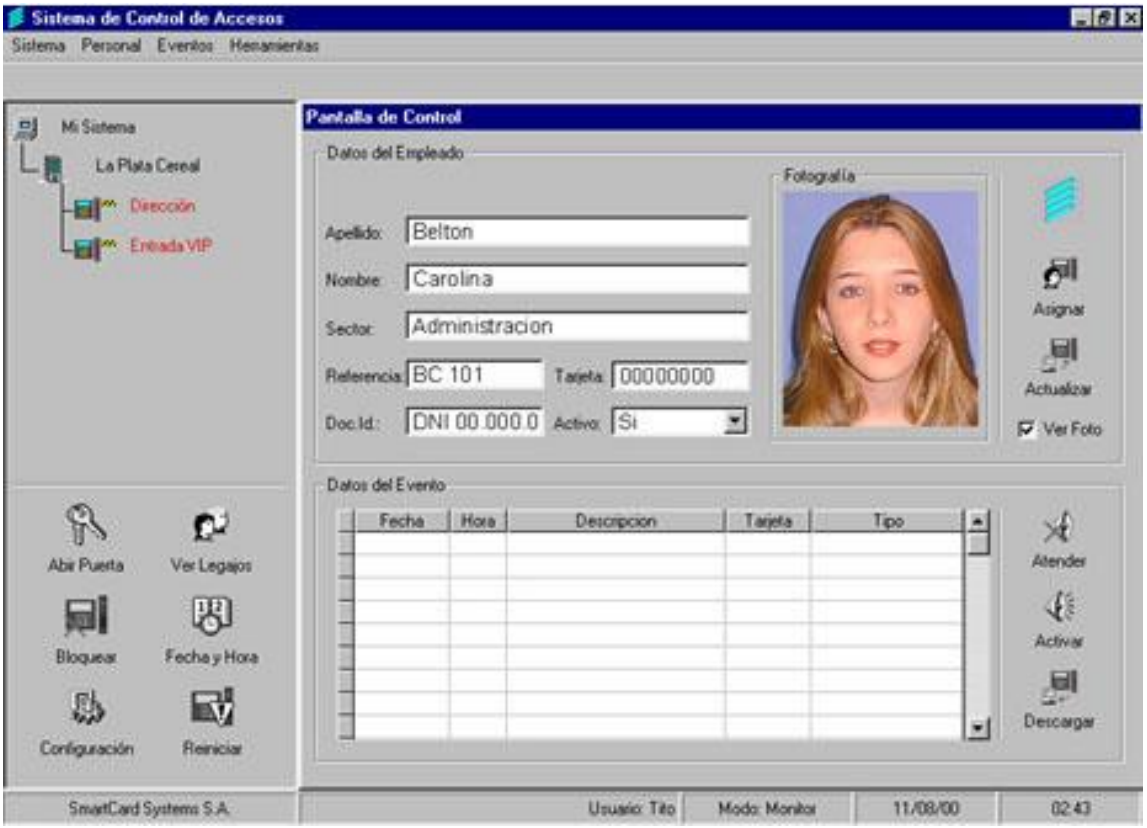
Todas las aplicaciones propias o desarrolladas fuera de la organización deben contar con un responsable de las contraseñas y este debe tener controladas todas las contraseñas que se extiendan a los usuarios de los sistemas en producción.

Las contraseñas deben estar codificadas y en una base de datos asegurada para evitar el robo o modificación de las mismas.

3.4.2. Accesos externos

Los accesos que se dan para ingresar a cualquier sistema de la organización desde una red externa deben estar revisados y aprobados por la coordinación de redes y telecomunicaciones, así como, por el jefe de área del empleado que puede ingresar, tomando en cuenta el tipo de permisos que se le conceden al empleado, así como, los privilegios que tiene para ingresar y sus alcances dentro del sistema.

Figura 48. **Sistema para control de accesos**



Fuente: Smartcard systems, controles de acceso. http://bit.ly/1HiD19V. Consulta: junio de 2015.

Debe existir una política bien clara respecto a los accesos desde el exterior a los sistemas de la institución, esto debido a que pueden representar un riesgo de seguridad muy grande por el hecho de dar accesos externos a personas sobre las que no se tiene mayor control.

Una de las maneras más eficaces de hacerlo es llevar un control de cada usuario asignado a través de sus datos personales, de los cuales se debe tratar de capturar la mayor cantidad posible para poder deducir responsabilidades a la hora de algún imprevisto o investigación respecto a incidentes de seguridad por violaciones externas.

3.5. Desarrollo y mantenimiento de los sistemas

Los sistemas o aplicaciones desarrolladas o contratadas por la organización deben cumplir con cuatro condiciones primordiales:

- Validación de datos de entrada
- Controles de procesamiento interno
- Autenticación de mensajes
- Validación de los datos de salida

Estas condiciones deben cumplirse para que la información que se maneje a través de dichas aplicaciones, no se vea comprometida por los accesos que se deben permitir para utilizar la aplicación principalmente si la aplicación se puede utilizar vía internet o en la red de la institución.

3.5.1. Mantenimiento preventivo

El mantenimiento preventivo debe estar contemplado dentro de los planes operativos de la organización y se debe tener especial cuidado en asignar los recursos necesarios para llevarlo a cabo periódicamente para así evitar posibles complicaciones de los sistemas, desembocando esto en potenciales pérdidas de información a través de la falla o inutilización de equipos por falta de mantenimiento y previsión.

Los mantenimientos periódicos a los equipos son muy poco considerados en los planes operativos de las empresas, porque se considera un gasto más que una inversión que no pareciera dar ningún fruto.

Los mantenimientos preventivos para los equipos de cómputo, representan un verdadero ahorro en costo, ya que esto previene fallas en los equipos que por su naturaleza son muy difíciles de reparar y por lo tanto se deben hacer reemplazos casi totales debido a que los dispositivos y equipos de cómputo están fabricados para funcionar hasta un cierto período de duración promedio y en cuanto presentan una falla grave es prácticamente imposible de reparar a menos que uno de sus componentes sea de fácil reemplazo y no afecte el funcionamiento del equipo completo.

3.5.2. Mantenimiento correctivo

Inevitablemente todos los sistemas, aunque se lleve un control estricto de mantenimiento preventivo, fallan por diversos factores, ya sea por la edad de los mismos, por imprevistos, por siniestros ocurridos en el área donde se encuentran, por accidentes laborales o bien por acciones malintencionadas de personas o grupos ajenos a la empresa.

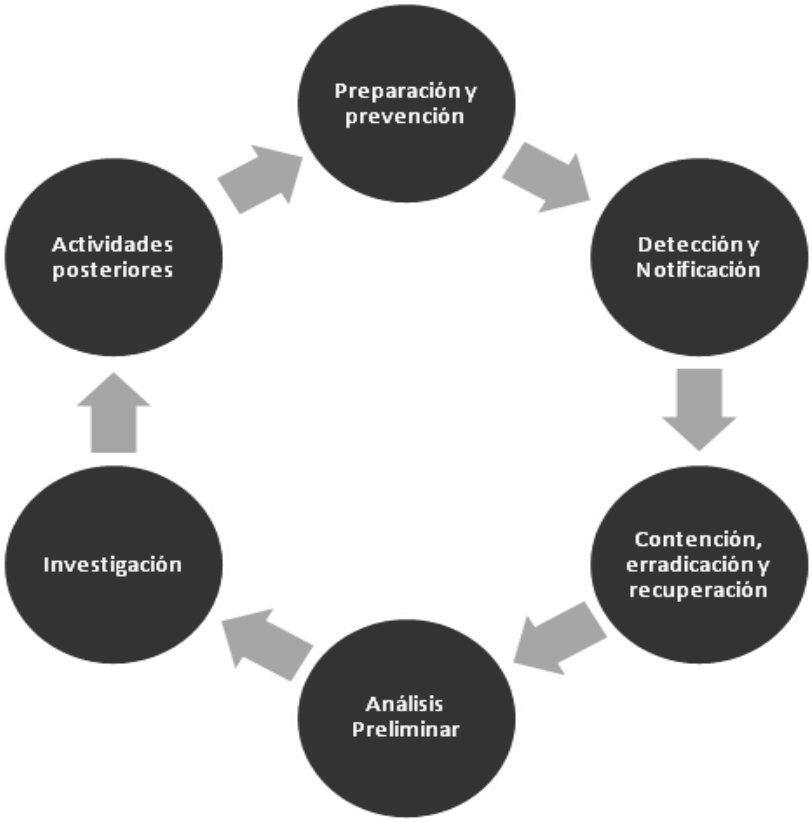
Por tales motivos la institución también debe destinar un fondo de previsión no solamente económico sino también en la medida de lo posible tener equipos de respaldo y que no comprometan el presupuesto, así como, procedimientos establecidos en caso de ocurrir algún imprevisto.

3.6. Gestión de incidentes de seguridad de la información

Un incidente de seguridad de información es un evento que puede comprometer las operaciones y funcionamiento de los sistemas tanto físicos como digitales de la organización. Esta clase de incidentes son iniciados por un evento o por una serie de eventos inesperados o indeseados que tienen una alta probabilidad de comprometer la seguridad de la información.

La gestión de incidentes de seguridad de información está basada principalmente en la asignación adecuada de recursos y su debido uso, con el objetivo de prevenir, detectar y corregir incidentes que puedan afectar la seguridad de la información de la institución. Una buena manera es utilizando una metodología simple para gestionar incidentes de seguridad.

Figura 49. **Metodología para gestionar incidentes de seguridad**



Fuente: elaboración propia.

Pero para que esta metodología se ponga en práctica, la institución debe hacer el esfuerzo por crear una unidad de manejo de incidentes de seguridad, por lo regular a esta unidad se le conoce como: CSIRT (Computer Security Incident Response Team) o Equipo de Respuesta a Incidentes de Seguridad de Información, el cual es un grupo que recibe, revisa y responde a informes y actividades sobre incidentes de seguridad en la institución. Sus miembros deben estar en las áreas donde se administra información importante.

3.6.1. Evaluar las vulnerabilidades del entorno

Pero para que esta metodología se ponga en práctica, la institución debe hacer el esfuerzo por crear una unidad de manejo de incidentes de seguridad, por lo regular a esta unidad se le conoce como: CSIRT (Computer Security Incident Response Team) o Equipo de Respuesta a Incidentes de Seguridad de Información, el cual es un grupo que recibe, revisa y responde a informes y actividades sobre incidentes de seguridad en la institución. Sus miembros deben estar en las áreas donde se administra información importante.

Las vulnerabilidades del entorno deben evaluarse tanto a nivel interno como externo para determinar los posibles fallos de seguridad que puedan comprometer la seguridad de la información.

3.6.1.1. A nivel interno

Las vulnerabilidades a nivel interno, deben evaluarse iniciando por equipos individuales, la infraestructura de red, los accesos físicos a las áreas delicadas y también los medios portátiles, tales como, memorias o discos compactos, con los cuales puedan cargar o sustraer información de la institución.

3.6.1.2. A nivel externo

A nivel externo, las vulnerabilidades pueden presentarse desde el mismo enlace a Internet por cualquier medio, ya sea por redes físicas o inalámbricas, así como el ingreso de personas no autorizadas, el trasporte de equipos desde y hacia dentro de la institución, las amenazas que pueden darse desde otras redes locales, códigos maliciosos (virus, troyanos, malware, etcétera), hackers y demás personajes que puedan comprometer la integridad de la información.

3.6.2. Comprobar equipos y aplicaciones

Los equipos y aplicaciones deben comprobarse desde antes de ponerlos a funcionar y deben estar constantemente evaluados por el personal que los administra u opera y durante su puesta en marcha para darle seguimiento a fallas de seguridad.

3.6.2.1. Pruebas de seguridad en equipos

Todos los equipos deben ser sometidos a pruebas de seguridad por parte de cada uno de los responsables para determinar si existen posibles agujeros de seguridad en las aplicaciones o en el propio equipo, ya sea porque se encuentra en una área física a la que se puede ingresar sin ninguna restricción o determinar si existen otras personas que puedan obtener información del equipo y bajo qué condiciones.

3.6.2.2. Pruebas de seguridad en aplicaciones

Las aplicaciones se deben someter a pruebas de seguridad basadas principalmente en las vulnerabilidades respecto a la transmisión de información, los accesos o autorizaciones, el alcance de las aplicaciones en cuanto a accesos remotos (internet, redes privadas o locales), para así determinar si es posible obtener acceso fácilmente, porque se debe tener una política en cuanto a los accesos remotos. Las aplicaciones son el medio más fácil para vulnerar la seguridad de la información de la institución porque las aplicaciones están vinculadas generalmente con información en bases de datos.

3.6.3. Establecer programas de formación sobre seguridad

La formación en seguridad se refiere principalmente a la creación de conciencia en el personal sobre asuntos que puedan vulnerar la seguridad de los ambientes, equipos, aplicaciones y dispositivos que contienen información valiosa de la organización.

Porque regularmente quienes saben o tienen entendidas las amenazas puede que tengan precauciones acerca de incidentes de seguridad pero no es así, por ejemplo, para empleados como secretarias, grabadores o digitadores, técnicos en áreas que no son informáticas pero que usan equipo digital, así como, profesionales y otros empleados que no estén debidamente instruidos en temas de seguridad informática.

3.6.4. Establecer directivas de seguridad en cuanto a contraseñas

Las directivas más importantes para el manejo de seguridad en cuanto a contraseñas pueden citarse a continuación:

- No utilizar la misma contraseña en todos los sistemas o servicios.

- No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, apellidos ni su fecha de nacimiento. Tampoco utilizar datos como el número de cédula, DPI o número de teléfono.

- No se deben utilizar secuencias básicas de teclado (por ejemplo:”abcd”, “qwerty” o las típicas: “12345” o “54321”).

- No repetir caracteres en la contraseña. (ejemplo: “9999”).

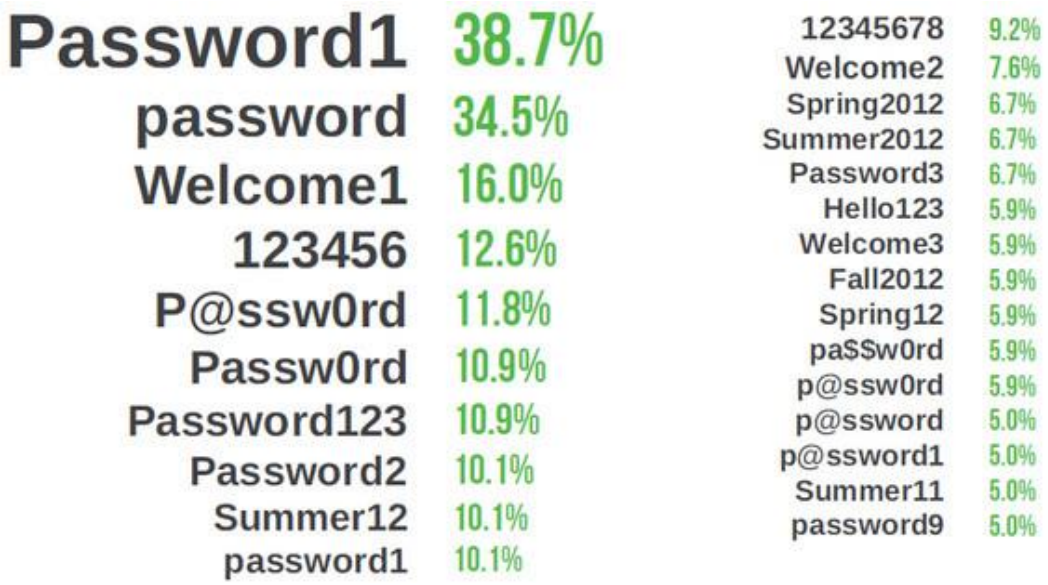
- Se debe evitar utilizar solamente números, letras mayúsculas o minúsculas.

- No se debe utilizar el nombre de usuario como contraseña, es decir, que de ninguna manera el nombre de usuario forme parte de la contraseña.

- No utilizar datos relacionados con el usuario que sean fácilmente deducibles o derivados de estos. (ejemplo: apodos, nombre de la pareja, el nombre de actor o personaje preferido, etcétera).

- Nunca dejar escrita en ninguna parte la contraseña. Tampoco guardar en documentos de texto en la computadora o dispositivo.

Figura 50. **Las peores contraseñas utilizadas en las empresas**



Fuente: MuySeguridad, seguridad informática. http://bit.ly/1HiF79M. Consulta: junio de 2015.

- No se debe utilizar palabras de diccionario, por ser fácilmente descifrables por sistemas especiales.

- Nunca enviar la contraseña por correo electrónico o en un mensaje de texto por celular.

- Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en cajeros automáticos y que el sistema se bloquee si se excede el número de intentos fallidos permitidos.

- No escribir las contraseñas en computadoras que se desconozca su nivel de seguridad y que puedan estar monitorizadas o en computadoras de uso público (bibliotecas, cibercafés, etcétera).

- Cambiar las contraseñas que por defecto son proporcionadas por desarrolladores/fabricantes de software.

Existen herramientas en internet que pueden ayudar a poder verificar si una contraseña es lo suficientemente segura para utilizarla, sobre todo en ambientes y sistemas que manejan información importante de la institución.

Se puede citar como ejemplo el sitio https://howsecureismypassword.net/ , ahí se puede hacer una comprobación muy sencilla para verificar si una contraseña es lo suficientemente segura. El sitio hace un análisis instantáneo de la contraseña ingresada y devuelve un mensaje indicándole al usuario el tiempo que un sistema para romper contraseñas tardaría para encontrarla.

Además, este sitio también hace recomendaciones sobre la manera óptima de crear una contraseña que no sea fácil de romper por sistemas o programas de hackers que son para esos fines.

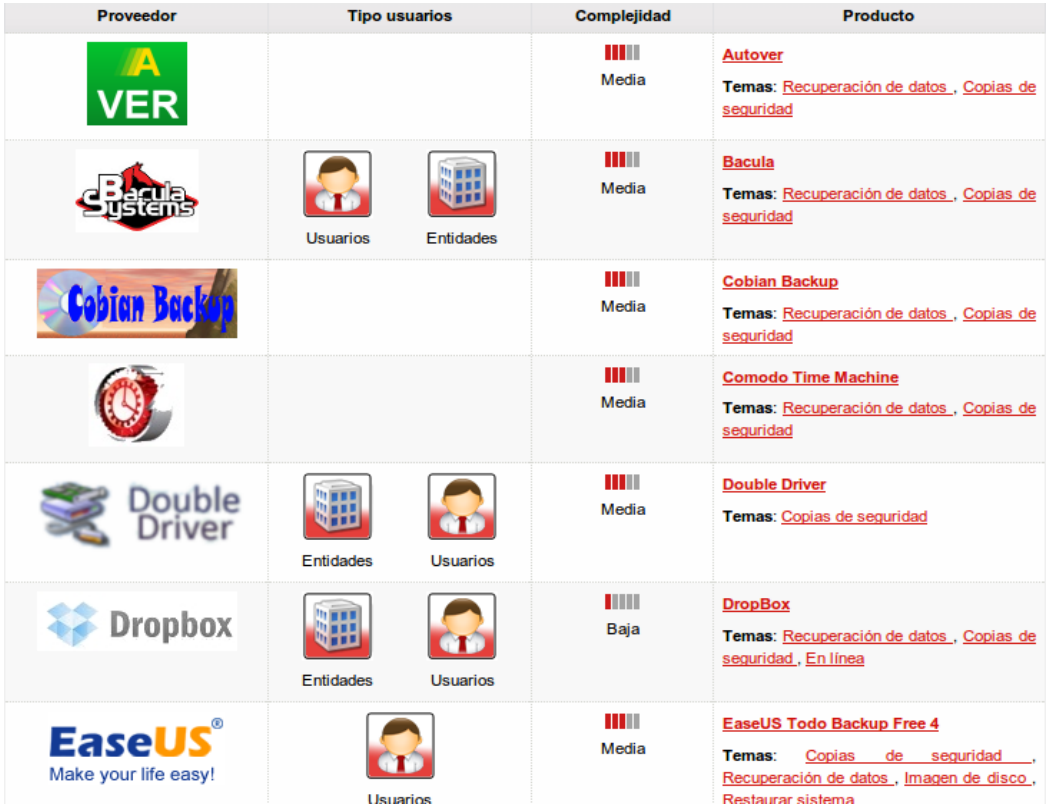
3.6.5. Comprobar los procedimientos de seguridad

Cuando se diseña una política de seguridad, una parte importante de su puesta en marcha debe ser la comprobación de los procedimientos establecidos para la seguridad de la información, esto debe llevarse a cabo por el personal técnico que tiene conocimiento de la infraestructura y dispositivos a ser puestos a prueba a través del procedimiento que se estableció para determinar si el procedimiento cumple con su cometido.

3.6.5.1. Copias de seguridad

Las copias de seguridad deben guardarse en medio magnéticos (discos duros, discos compactos, DVD, cintas magnéticas) que puedan utilizarse posteriormente para restaurar el original después de una eventual pérdida de datos ya sea por algún siniestro o bien por la corrupción de datos por cualquier razón indeseada.

Figura 51. **Ejemplos de herramientas gratuitas para copias de seguridad**



Proveedor	Tipo usuarios	Complejidad	Producto
AVER		Media	**Autover** **Temas**: Recuperación de datos , Copias de seguridad
Bacula Systems	Usuarios, Entidades	Media	**Bacula** **Temas**: Recuperación de datos , Copias de seguridad
Cobian Backup		Media	**Cobian Backup** **Temas**: Recuperación de datos , Copias de seguridad
		Media	**Comodo Time Machine** **Temas**: Recuperación de datos , Copias de seguridad
Double Driver	Entidades, Usuarios	Media	**Double Driver** **Temas**: Copias de seguridad
Dropbox	Entidades, Usuarios	Baja	**DropBox** **Temas**: Recuperación de datos , Copias de seguridad , En línea
EaseUS Make your life easy!	Usuarios	Media	**EaseUS Todo Backup Free 4** **Temas**: Copias de seguridad , Recuperación de datos , Imagen de disco , Restaurar sistema

Fuente: INTECO. http://bit.ly/KfFyVK. Consulta: abril de 2012.

3.6.5.2. Restauración

La restauración es el procedimiento por medio del cual se recupera información digital que fue previamente almacenada y que se tenía como respaldo a la hora de querer restaurar un sistema a su estado original, o al menos a un estado cercano al más reciente para continuar las actividades normales de la empresa o institución.

4. IMPLEMENTACIÓN DE LA PROPUESTA

4.1. Marco gerencial para la implementación del plan

La gerencia debe establecer un esquema para que las políticas sean un esfuerzo conjunto entre todos los empleados involucrados. También se deben comunicar y poner a disposición de todos los empleados y de una manera accesible, el contenido de las políticas, los documentos relacionados a la misma y también se debe motivar e inspirar al equipo para cuidar los activos de la empresa a través de su trabajo responsable y apegado a las políticas de seguridad de información.

4.1.1. Difundir los objetivos y prioridades de la propuesta

Los objetivos y prioridades deben estar plasmados en un documento a la vista de todos, o bien, distribuirse a todo el personal para que estos se concienticen de las responsabilidades que tienen respecto a las políticas de seguridad y su relación con las actividades que realizan dentro de la organización.

4.1.2. Delegar funciones y responsabilidades

Las funciones y responsabilidades deben estar plasmadas en un documento que debe ser de fácil acceso, así como, cada coordinador de área debe tener definidas las responsabilidades y tareas de cada colaborador del área que dirige, también debe regir de acuerdo a las directrices establecidas en el Plan Operativo Anual (POA).

4.1.2.1. Mandos medios

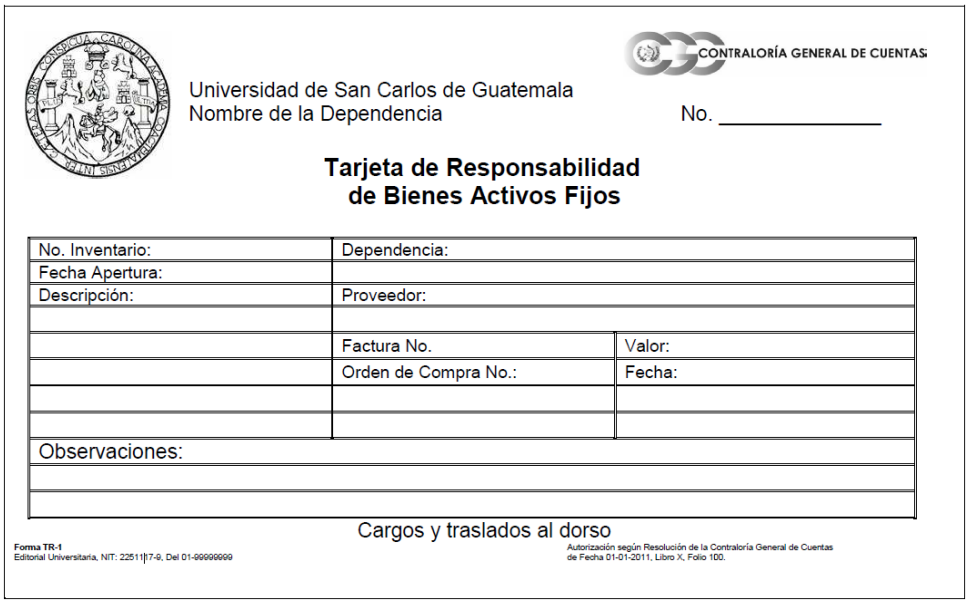
Los mandos medios se refieren en este caso particular a los profesionales en cada área bajo el mando de la jefatura, o bien, los coordinadores que delegarán las funciones y responsabilidades a los colaboradores de la institución, aportando su experiencia y conocimiento en el manejo de situaciones de alto riesgo en materia de seguridad de la información. Ellos deben ser el enlace principal entre las políticas de seguridad de información, la jefatura, los involucrados en el manejo de información, clientes internos y externos de la institución para lograr una cohesión entre los actores y el cumplimiento de lo establecido en las políticas.

4.1.2.2. Responsables de equipos

Cada equipo debe estar debidamente etiquetado e identificado, así como, tener asociada una tarjeta de responsabilidad con el nombre y el registro o número de personal del empleado, para saber en cualquier momento bajo la tutela de quién se encuentra, también el historial de traslados que ha sufrido dicho equipo, para determinar la responsabilidad en caso de situaciones de riesgo.

Los equipos deben tener un número único para ser identificados, esto de acuerdo a los estándares del sistema de clasificación adoptado por la organización, dichos equipos deben tener un historial sobre los responsables que han tenido a lo largo de su vida útil. Las tarjetas de responsabilidad son un medio muy fiable para llevar el control de los equipos dentro de una organización e incluso se puede saber quiénes han sido responsables de su uso.

Figura 52. **Tarjeta de responsabilidad de bienes (anverso)**



CONTRALORÍA GENERAL DE CUENTAS

Universidad de San Carlos de Guatemala
Nombre de la Dependencia

No. _____

Tarjeta de Responsabilidad de Bienes Activos Fijos

No. Inventario:	Dependencia:	
Fecha Apertura:		
Descripción:	Proveedor:	
	Factura No.	Valor:
	Orden de Compra No.:	Fecha:
Observaciones:		

Cargos y traslados al dorso

Forma TR-1
Editorial Universitaria, NIT: 2251117-9, Del 01-99999999

Autorización según Resolución de la Contraloría General de Cuentas de Fecha 01-01-2011, Libro X, Folio 100.

Fuente: elaboración propia.

Figura 53. **Tarjeta de responsabilidad de bienes (reverso)**

Traslados

Fecha	Pasa a:	Autorización

Cargos

Fecha	Recibí conforme	
	Nombre	Firma

Forma TR-1
Editorial Universitaria, NIT: 2251117-9, Del 01-99999999

Autorización según Resolución de la Contraloría General de Cuentas de Fecha 01-01-2011, Libro X, Folio 100.

Fuente: elaboración propia.

4.1.2.3. Responsables de aplicaciones

Las aplicaciones deben estar inventariadas de acuerdo a los responsables involucrados desde el diseño, creación, puesta en marcha y mantenimientos, así como, los usuarios y sus respectivas contraseñas para determinar en cualquier momento a través de las bitácoras de los mismos, todos los accesos y movimientos efectuados con la información a través de los usuarios y administradores del sistema.

4.1.3. Estimular la participación de los colaboradores

Las actividades colectivas generan la participación y colaboración del grupo de empleados, si éstas se llevan a cabo de una manera ordenada y con coordinación de la jefatura para oficializar las actividades o bien organizar estas actividades de acuerdo a un calendario, es decir, periódicamente para que se pueda dar seguimiento a dichas actividades y que generen participación activa en un plazo determinado.

4.2. Niveles de protección y medidas para el tratamiento de la información

La información que se maneja en la institución debe tener medidas claras para la protección de la información, debiendo tener identificados claramente los niveles de seguridad, estos normalmente van desde la seguridad física, seguridad a nivel de aplicaciones y seguridad a nivel de usuarios.

4.2.1. Seguridad a través de equipos

La seguridad a través de los equipos debe estar diseñada tomando en cuenta dos importantes aspectos: los niveles de seguridad y las prácticas para la seguridad de los mismos.

4.2.1.1. Niveles apropiados de seguridad para los equipos

Dependiendo de la importancia de la información contenida en los equipos, la seguridad debe implementarse en esa medida, es decir, si la información no es muy relevante, con un mínimo de seguridad estará bien resguardada y aunque pudiera comprometerse de alguna manera esa información, no es de gran preocupación. Por otro lado, si la información en cuestión es de suma importancia, se deben tener niveles de seguridad apropiados y acorde a la trascendencia de la misma.

Estos niveles pueden ir desde la utilización de la codificación o encriptación de las contraseñas guardadas, el uso de certificados de seguridad si esta información se debe capturar o presentar en un sitio de Internet, así como, un control estricto de los roles y contraseñas bajo la política y directivas de la institución.

4.2.1.2. Prácticas de seguridad para equipos

Las prácticas de seguridad más importantes que se deben verificar para el aseguramiento de los equipos son: prevenir o evitar accesos no autorizados, daños o intrusión a los ambientes, instalaciones e información de la organización.

Proteger el equipo que procesa información crítica de la organización ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad, todo ello con medidas de seguridad y controles de acceso adecuados.

Asimismo, se debe tomar en cuenta la protección del mismo si existiera un traslado o durante la permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

También se deben controlar factores ambientales que puedan entorpecer el funcionamiento normal de los equipos informáticos que guardan la información de la organización, tales como siniestros, posibles ataques por personas sin escrúpulos y medidas para la protección de la información que maneja el personal de las oficinas en el desempeño de sus labores habituales.

4.2.2. A nivel de aplicaciones

Una de las razones del por qué en una organización, las aplicaciones están bajo muy pocos controles de seguridad es porque prácticamente se hace imposible que la gente que trabaja directamente en seguridad se involucre en el desarrollo o mantenimiento de aplicaciones, entonces esta separación se hace porque la operación y el servicio es primero.

Entonces para ello se debe buscar un enlace entre el equipo de seguridad y el equipo de desarrollo de sistemas para que estén de acuerdo sobre los niveles de seguridad que se deben tratar y los controles que deben respetarse y también los que deben implementarse si estos no existieran.

4.2.2.1. Niveles apropiados de seguridad para aplicaciones

Los niveles apropiados para asegurar las aplicaciones en la organización pueden enumerarse, aunque pueden ser muchos los momentos y lugares donde puede ocurrir un incidente que amenace la seguridad de la información.

Estos niveles de seguridad se dividen en cuatro principales grupos:

- Sistema operacional: es decir la plataforma o Sistema Operativo que se tiene instalado.

- Comunicaciones: la infraestructura de red tanto a nivel local como las conexiones remotas incluida la Internet.

- Almacenamiento de datos: los repositorios de datos o almacenes de datos deben tener niveles de protección adecuados y acorde a la importancia y el tamaño de la información que se almacena en ellos.

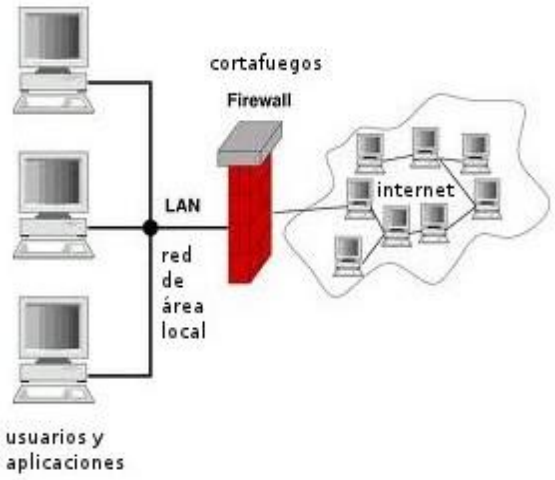
- Entorno de la aplicación: no sólo se refiere al entorno lógico o digital sino también al entorno físico, tanto a nivel de equipo de cómputo como a empleados.

4.2.2.2. Prácticas de seguridad para aplicaciones

A nivel operacional, es indispensable utilizar sistemas de protección local tales como: antivirus o *firewalls*, hacer de carácter obligatorio el uso de contraseñas bajo una política establecida para restringir el acceso a los sistemas y utilizar aplicaciones para habilitar esta funcionalidad.

Deshabilitar todas las acciones automáticas de los sistemas en producción, tales como el desvío de mensajes, envío de mensajes remotos, apertura de conexiones, ventanas separadas, envío de datos sin codificar y sobre todo, no permitir que los sistemas arranquen automáticamente sin el uso de contraseñas.

Figura 54. **Esquema básico de seguridad con cortafuegos**



Fuente: elaboración propia.

A nivel de comunicaciones, deshabilitar servicios que no sean necesarios, deshabilitar conexiones de redes físicas e inalámbricas que no se estén utilizando, usar un mecanismo de cifrado para almacenar datos sensibles como contraseñas, utilizar en la medida de lo posible sitios y aplicaciones con seguridad HTTPS en lugar de HTTP, emplear esquemas de autenticación robustos como RADIUS o LDAP.

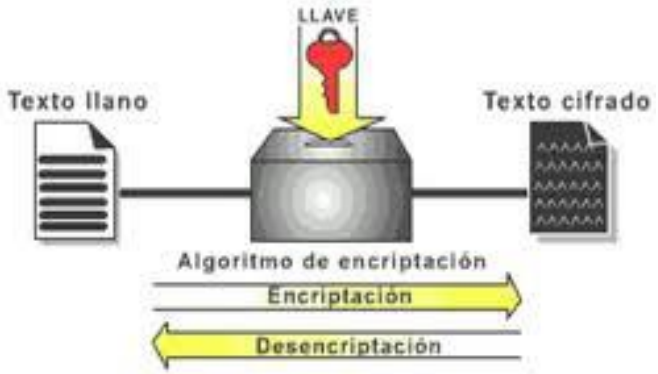
Para tener confianza en un sitio de Internet que maneje datos sensibles (bancos, sitios de compra por Internet, empresas que manejan información confidencial, etcétera) se debe tener en cuenta que cuando se navega por esos sitios se debe verificar que en la dirección tenga antepuesto: https:// y que el navegador muestra un ícono con un candado que indica la seguridad aplicada al sitio, si el protocolo es http:// , quiere decir que la dirección de la compañía o institución no es totalmente confiable y por lo tanto, podría ser objeto de un fraude o robo de información.

Figura 55. **Protocolo de navegación segura HTTPS**

Fuente: Culturacion, seguridad informática. http://bit.ly/IHXsQK. Consulta: junio de 2015.

A nivel de almacenamiento de datos, estos deben estar en áreas físicas seguras, con la mínima exposición a desastres de origen fortuito como incendios, inundaciones y temperaturas extremas. Por otra parte, a nivel de software, los datos deben estar almacenados bajo un sistema de cifrado, el cual debe garantizar que la información aun siendo extraída, no podrá ser leída de forma directa por personas ajenas.

Figura 56. **Cifrado de datos**



Fuente: RÍOS, Julio. Seguridad informática, cifrados de datos. http://bit.ly/IYxNQZ. Consulta: junio de 2015.

A nivel del entorno de las aplicaciones, proteger los recursos remotos que las soportan contra posibles ataques (aplicaciones e infraestructura), descargar aplicaciones de terceros sólo desde sitios confiables y preferiblemente firmadas de forma digital, utilizar prácticas de programación segura, esto último debe ser una política bien definida para el desarrollo de aplicaciones propias de la organización, ya que se debe involucrar al equipo encargado de la seguridad y al equipo encargado del desarrollo de las mismas.

4.2.3. A nivel de usuarios

La seguridad a nivel de usuarios, también llamada seguridad lógica, consiste en la aplicación de barreras y procedimientos que mantengan resguardados los accesos a la información restringida de la organización y que sólo se permita acceder a las personas que tienen la debida autorización para hacerlo. Se deben establecer normas que eliminen o bien minimicen los riesgos para la información o la infraestructura informática de la institución.

Dichas normas deben incluir horarios de trabajo, restricción de acceso a determinados lugares, autorizaciones, denegaciones, perfiles, roles, planes de contingencia, procedimientos y protocolos, así como, todo lo necesario que permita un buen nivel de seguridad, minimizando el impacto en el funcionamiento de la institución y el desempeño de los empleados.

4.2.3.1. Acceso a los equipos

Los equipos tanto a nivel físico como lógico solamente deben ser utilizados por las personas que están designadas y bajo contrato de la institución, porque de suceder un evento dañino, la persona que tiene designado el equipo y las aplicaciones que este contiene, debe ser sancionado, de acuerdo a los reglamentos internos de la institución, de ser necesario y si la gravedad del caso lo amerita se deben tomar acciones legales para el caso.

4.2.3.2. Acceso a las aplicaciones

Una aplicación que no tiene niveles de seguridad mínimos para acceder a ella es un potencial agujero de seguridad que puede comprometer no solamente la información contenida en ella, sino también puede dar paso a que se pueda acceder a otras áreas del sistema y comprometer información aún más delicada.

Los accesos deben estar custodiados por alguno de los mandos medios o bien desde la jefatura, de acuerdo a un esquema de seguridad que se debe establecer y que cada colaborador debe conocer, debido a las responsabilidades que conlleva tener una aplicación abierta y no estar en su puesto de trabajo, dejar contraseñas escritas en lugares visibles.

Compartir información que está bajo su responsabilidad con otros empleados o bien con personas externas y también prestar o ceder el equipo a otras personas sin tomar las debidas medidas de precaución.

4.2.3.3. Buenas prácticas de seguridad para usuarios

Uno de los mecanismos más fiables que se puede implementar para reducir problemas relacionados a la seguridad informática, es la implementación de un programa de sensibilización en seguridad informática.

En conjunto con las subjefaturas, el jefe debe plasmar las medidas básicas para seguridad de equipos y aplicaciones, así como, implementar medidas para ingresar a las áreas físicas que son delicadas en la institución, un inventario de aplicaciones, usuarios, roles y permisos para que sea fácil detectar intrusiones o bien ataques internos o externos, así como, los procedimientos para dar de alta/baja a un usuario en los diferentes sistemas y aplicaciones debido a despidos, renuncias, cambio de cargos, traslados, etcétera.

4.3. Reducción de riesgos

Los riegos se pueden reducir con: guardias de seguridad para áreas físicas, programas de seguridad para los empleados, control de usuarios, control de aplicaciones, realización periódica de copias de seguridad, alarmas y estimación de futuras pérdidas con la asesoría de expertos.

4.3.1. Control de usuarios y procesos

Los usuarios deben estar debidamente identificados dentro de los sistemas y aplicaciones, esto con el fin de evitar dualidad de identificaciones, por ello, cada usuario que se habilite en los sistemas debe estar identificado y tener los permisos necesarios para sus tareas asignadas dentro de dichos sistemas y estos deberán ser intransferibles. Los procesos que lleva a cabo cada colaborador en la institución deben ser supervisados constantemente no solamente para evaluación de desempeño sino también para evitar que, por ejemplo, las contraseñas o bien la información sea compartida entre empleados.

Recomendaciones importantes:

- Llevar control y registro de todas las transacciones hechas en las diferentes aplicaciones de la institución, este control se debe realizar por cada usuario.

- Se debe limitar el acceso a los módulos de los sistemas según el perfil de cada usuario.

- Utilizar protocolos estándares de autenticación y métodos para evitar intrusiones, tales como, utilizar un número limitado de intentos fallidos en el ingreso a los sistemas, por ejemplo, si el usuario ingresa 3 veces incorrectamente su información de autenticación, entonces el sistema deberá bloquearle el acceso por un determinado tiempo.

- Control de acceso a la información según el perfil del usuario.

- Esto para evitar que un usuario de otra aplicación ingrese en el perfil de otro usuario y pueda llevar a cabo funciones que no le corresponden.

- Control de la edición (ingreso, modificación y eliminación) según el perfil del usuario.

Cada usuario deberá tener acceso a ciertos privilegios, por ejemplo, si se trata de un grabador de información, un programador, un administrador de sistema, el jefe o una secretaria, cada uno deberá tener privilegios distintos de acuerdo a su perfil laboral y también a su rol y perfil en los sistemas en que participa.

Ejemplo de niveles de acceso para usuarios por aplicaciones:

Nivel 1: ver o imprimir datos comunes

Nivel 2: para ingresar datos comunes

Nivel 3: permite modificar datos comunes

Nivel 4: se pueden eliminar datos comunes

Nivel 5: ver o imprimir datos confidenciales

Nivel 6: ingresar datos confidenciales

Nivel 7: modificar datos confidenciales

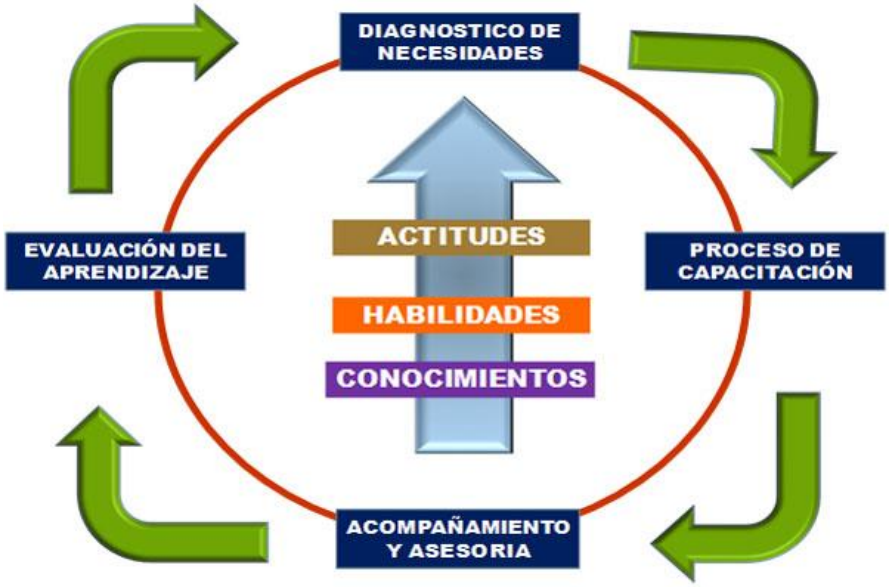
Nivel 8: eliminar datos confidenciales

Nivel 9: es el nivel de auditoría o administración general del sistema

4.3.2. Formación continua

Uno de los aspectos que se descuida mucho luego de definir políticas, es que, pasado cierto tiempo no se realimentan los procesos ni se realizan cuestionamientos ni evaluaciones sobre el funcionamiento de las mismas, esto con el fin de lograr una formación constante en los colaboradores en caso de existir dudas o planteamientos que puedan beneficiar a la institución.

Figura 57. **Metodología de formación continua**



Fuente: Escuela de formación continua, Perú. http://bit.ly/1g3tZ6E. Consulta: junio de 2015.

Así también, es de suma importancia no solo la capacitación y formación desde adentro, sino también se deben contratar expertos en materia de seguridad para mantener las políticas acorde a los tiempos.

Para llevar a cabo un programa de formación continua en el departamento, se debe iniciar con determinar en las 3 diferentes coordinaciones: Análisis y Desarrollo, Redes y Desarrollo Web, los principales actores en los sistemas más importantes que tiene bajo su tutela el departamento.

Por ejemplo, si un empleado es experto en una determinada área y hay otros que trabajan en el mismo sistema, se debe seleccionar como instructor a ese empleado experimentado o con mayores conocimientos y habilidades, para que él se encargue de la formación de sus compañeros, para así, mejorar las habilidades y conocimientos de sus compañeros, esto traerá consigo beneficios importantes como son: ahorro en tutorías externas, aumento de las competencias de los empleados y plusvalía para los trabajadores al adquirir más conocimiento de los procesos y sistemas del departamento.

Por otra parte, es importante la inversión del departamento en la formación de sus empleados, principalmente en un Departamento de Tecnología, los sistemas actuales sufren cambios en muy corto tiempo y la formación continua es una carrera constante, para ello se debe invertir en formación, capacitación interna y externa, certificación de conocimientos, utilización de un beneficio muy importante que brinda la Universidad de San Carlos, el cual es brindar a sus empleados un espacio de tiempo para continuar su formación académica y en aras de mejorar su desempeño laboral, optar a mejores cargos, ascensos, aumentos de sueldo y promociones.

En algunos casos, traslado a otras dependencias que necesitan de personal capacitado y que ya tiene experiencia laboral dentro de la misma institución. Todo esto también incidirá en la reducción de riesgos en el manejo de información ya que al adquirir más y mejores conocimientos, los empleados tendrán mayor control y mucho más cuidado en el manejo de la información de la institución.

4.3.3. Clasificación de la información

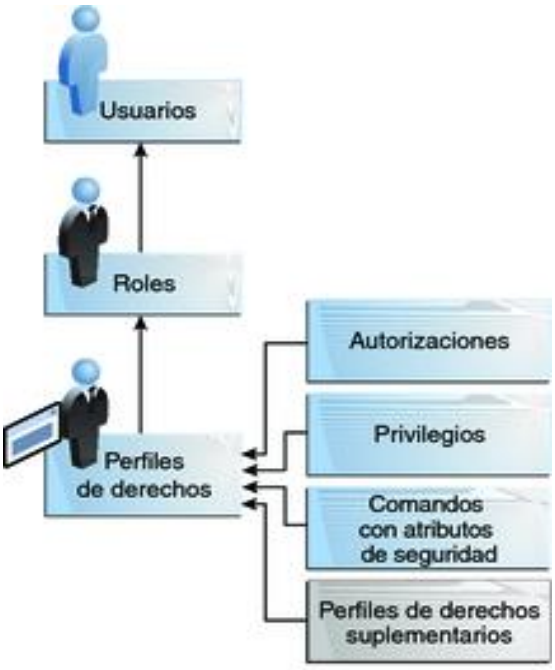
La clasificación de la información consiste básicamente en saber de qué información dispone la institución, cuál es la mejor manera de manipularla, cuál debe desecharse, qué lugares y en qué dispositivos debe guardarse, así como, definir claramente los métodos y procedimientos para recuperarla en caso fuera necesario restablecer copias de seguridad, sustitución o migración de datos desde otros sistemas o adaptación de información proveniente de fuentes externas.

4.3.4. Autorizaciones basadas en roles

Todos los accesos que se den a los usuarios registrados en las bases de datos de la institución y que están contratados para realizar determinadas tareas, deben estar justificados y clasificados debidamente, basados en el rol que juega el usuario dentro de los sistemas de la institución.

Por ejemplo, una persona que realiza consultas de información sobre empleados sólo para revisión y no tiene permisos de modificar dicha información, no puede ni debe dársele acceso para esta última operación debido a que la información personal de los empleados debe ser manipulada únicamente por los mismos empleados o bien, por profesionales que se dediquen a realizar procesos sobre recursos humanos y que tengan ese rol dentro del sistema y esté definido en su perfil laboral.

Figura 58. **Seguridad basada en roles**

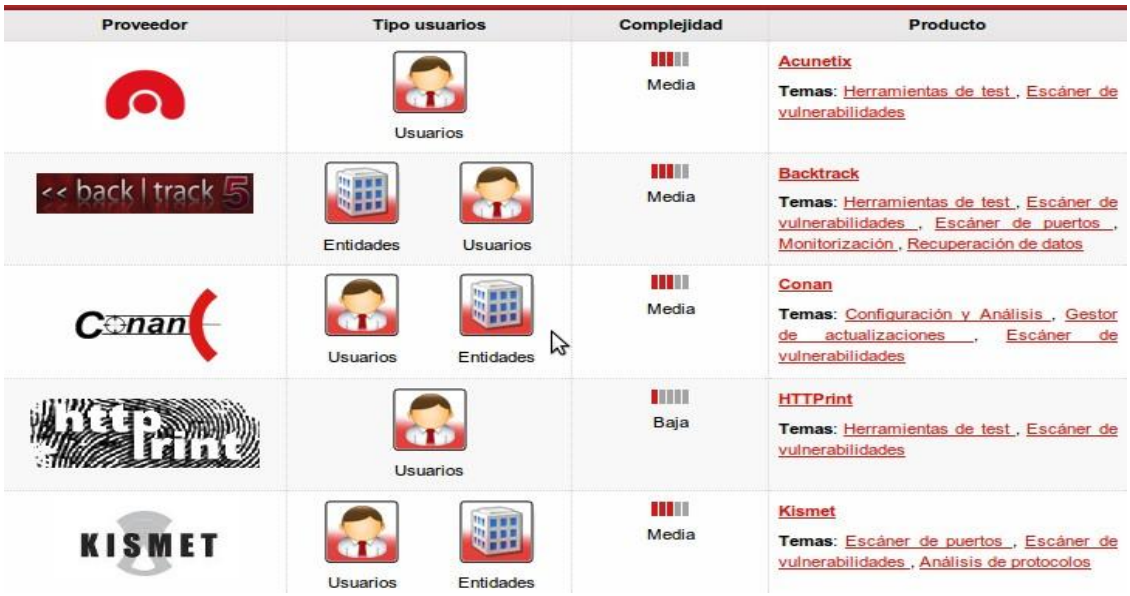


Fuente: Oracle, servicios de seguridad. http://bit.ly/IxHrLW. Consulta: junio de 2015.

4.3.5. Registro de ataques y amenazas

Todos los eventos que ocurren en los sistemas y equipos, deben ser debidamente identificados y documentados por parte del equipo de respuesta a incidentes de seguridad, esto con el fin de llevar un registro estadístico no solamente como una bitácora de eventos, sino también para analizar estadísticas sobre ataques y vulnerabilidades que puedan tener los sistemas de seguridad que están implementados.

Figura 59. **Algunas herramientas para análisis de vulnerabilidades**



Fuente: Instituto Nacional de Tecnologías de Comunicación (INTECO), http://bit.ly/JWAaGS. Consulta: junio de 2015.

Se pueden utilizar diversas herramientas informáticas para hacer un análisis de vulnerabilidades y posibles fallas de seguridad, esto comprende entre otras cosas, análisis de páginas de Internet propiedad de la institución, aplicaciones web publicadas, gestión de actualizaciones de software, análisis de protocolos de red, análisis de servidores web, puntos de acceso a la red inalámbrica, *routers, switches, hubs, modems*, tráfico en la red y detección de intrusos.

Figura 60. **Incendio en centro de cómputo**

Fuente: LEAL, Christian. Allway Sync. http://bit.ly/JlWeIl. Consulta: junio de 2015.

Para ilustrar se va a suponer que la institución no tiene sistemas de detección ni de protección contra incendios en el cuarto de servidores. El coordinador del área de Redes o alguno de sus colaboradores deja unos papeles cerca o sobre el aire acondicionado, del área. Por la noche, dicho acondicionador se sobrecalienta y provoca un incendio que destruye una buena parte o toda el área de servidores y quizá algún área contigua.

Directivas:

Predecir ataque/riesgo: incendio
Amenaza: desastre natural, incendio
Ataque: no existe

Estrategia proactiva:

- Predecir posibles daños: pérdida de equipos e información
- Determinar y minimizar vulnerabilidades: protección contra incendios
- Evaluar planes de contingencia: copia de seguridad de la información

Estrategia reactiva:

- Evaluar daños: perdida de hardware e información.
- Determinar su origen y repararlos: bloqueo del aire acondicionado.
- Documentar y aprender.
- Implementar plan de contingencia: recuperar copias de seguridad y restaurarlas.

Los resultados obtenidos se deben analizar junto con la eficacia de la directiva: con esta información se deberá ajustar la directiva con los nuevos conceptos incorporados para retroalimentar la política de seguridad que está en vigencia, para evitar que vuelva a suceder un siniestro de ese tipo.

4.3.6. Responsabilidades para datos privados

Si existen roles dentro de la organización que involucren el manejo de información delicada, deben existir procedimientos documentados para realizar gestiones sobre información importante, de tal manera que si el empleado debe hacer cambios, se debe documentar y dejar constancia del cambio realizado o si el dueño de la información (si se trata de empleados u otras dependencias) solicita un cambio, modificación o eliminación de ciertos registros, debe justificar a través de una nota dirigida a la jefatura o la oficina encargada de manipular dicha información para que se haga efectivo el cambio o modificación, que previamente debe ser analizado.

Luego, se realizará la operación solicitada y se dejará un registro con los datos del usuario que lo realizó, quien lo solicitó, fecha, hora, motivo y lugar de la solicitud para llevar un registro de cambios en los sistemas.

4.4. Medidas de protección a la información

Se deben implementar medidas de protección a toda la información y de acuerdo a su importancia deben realizarse procesos de protección, manuales para su manipulación y que todos los empleados tengan claro que existe la documentación adecuada para realizar cualquier operación sobre los datos que posee la institución.

4.4.1. Catálogos de información

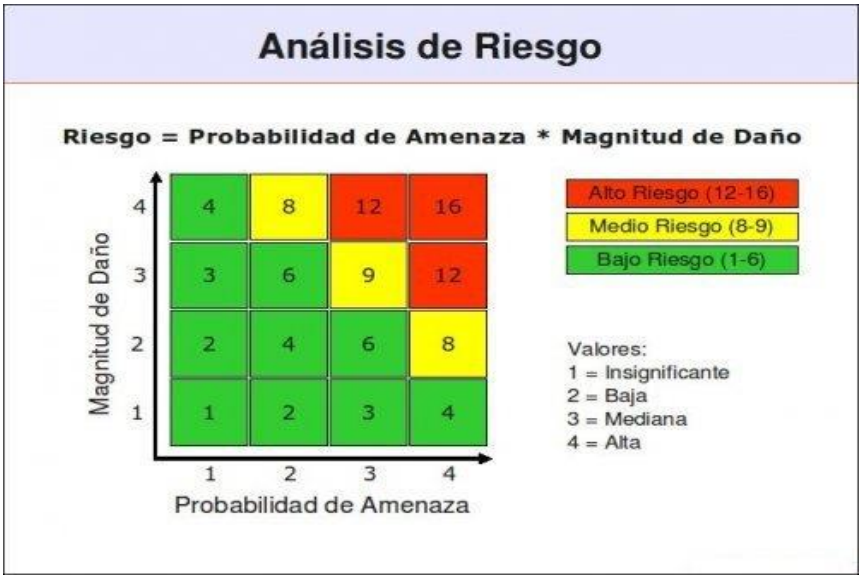
Los catálogos de información no son más que inventarios de los diferentes bancos de datos que maneja la organización. Estos deben estar clasificados con base a su importancia, el lugar donde se almacena, el tipo de dispositivo y el o los responsables de dichos catálogos.

4.4.1.1. Clasificación de información

A criterio de la jefatura y de acuerdo a la importancia de la información, se debe establecer una clasificación de las mismas por niveles de riesgo para la empresa, por ejemplo, asignar un color, una numeración o bien una codificación para identificar el nivel de importancia que pueda tener la información de acuerdo a una escala determinada para hacer más fácil la nomenclatura.

Una matriz de riesgo es una herramienta muy práctica para identificar, clasificar y ponderar de acuerdo a un criterio acordado entre la jefatura y las coordinaciones de área, para así tener un estándar a la hora de elaborar una matriz de esa naturaleza.

Figura 61. **Matriz para análisis de riesgo**



Fuente: Gestión de riesgo en seguridad informática. http://bit.ly/IpiB2U. Consulta: junio de 2015.

4.4.1.2. Lugares donde se almacena la información

Los lugares donde se almacena la información deben estar plenamente identificados y en cada coordinación debe tenerse un mapa con las ubicaciones físicas de las áreas donde se encuentran las bases de datos y repositorios de información para saber su ubicación en cualquier momento.

4.4.1.3. Responsables

Así como, se debe tener un inventario de equipos, se debe tener un inventario de responsables de los equipos y de las diferentes aplicaciones con que cuenta la organización. Las tarjetas de responsabilidad cumplen el papel de llevar un control de los equipos físicos y sus responsables.

Aunque para las aplicaciones, cada coordinación debería tener un inventario de las mismas y llevar el control de los responsables de la información que en ellas se maneja.

4.4.2. Análisis de impacto

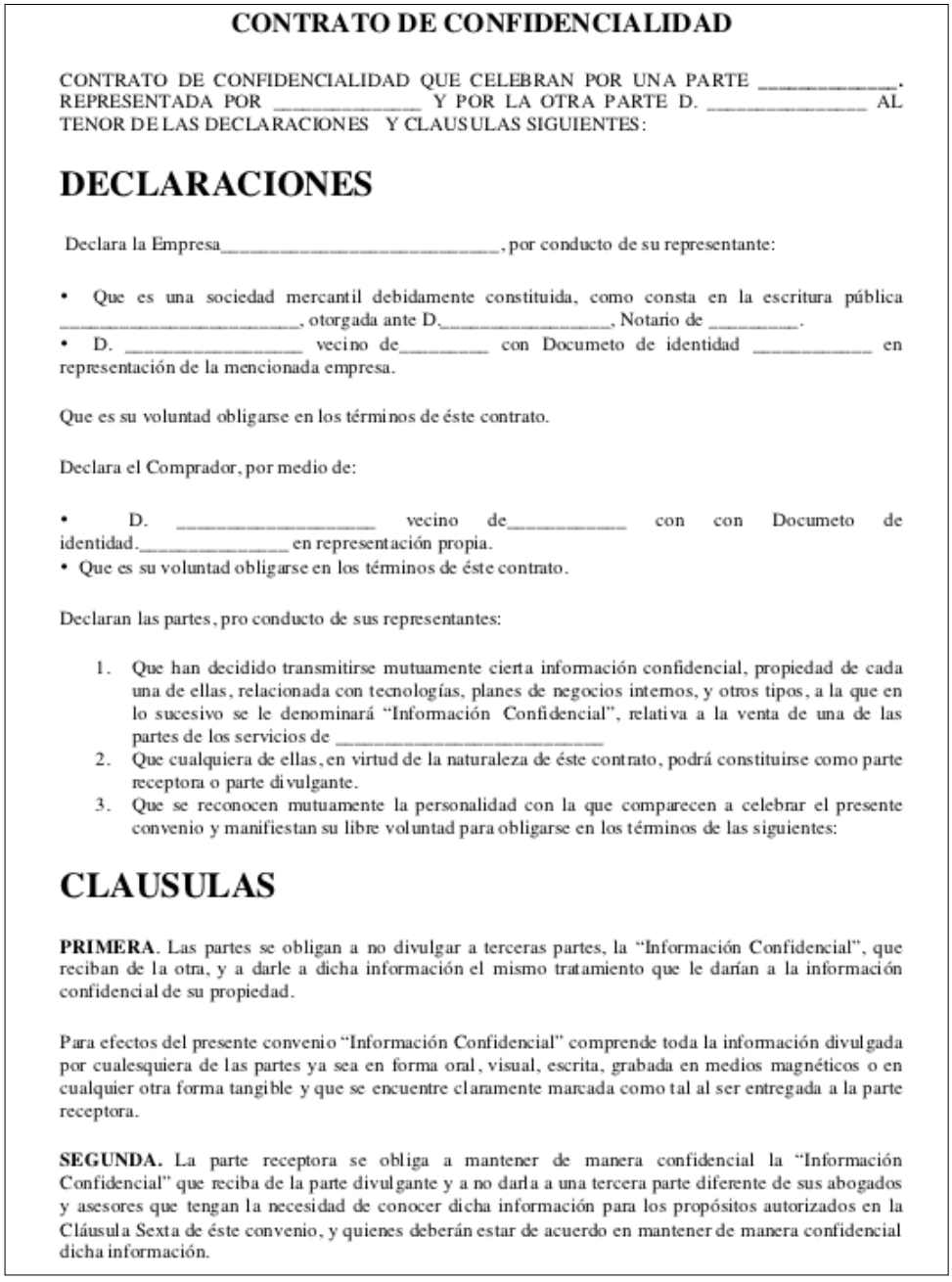
Uno de los retos de la política de seguridad de información, es asignar a través de una estrategia, los recursos físicos, económicos, humanos y tecnológicos para resguardar la información de la institución, esto se hace desde la identificación de los riesgos a los que está expuesta la institución, para con ello determinar el nivel de impacto que podrían tener esos riesgos de convertirse en un evento negativo para la institución. A partir de ello se debe elaborar una matriz de riesgo y si es posible, crear una escala para los niveles de impacto de los riesgos analizados.

4.4.2.1. Confidencialidad de la información

La información que posee la institución no importa su naturaleza, procedencia o importancia, debe ser tratada con sumo cuidado y con base al principio de confidencialidad, el cual dicta que la información únicamente debe ser conocida y manipulada por personas contratadas y autorizadas para dicho fin.

Dentro de las políticas de seguridad de información debe existir un reglamento disciplinario para todos los empleados en relación a sanciones administrativas e incluso legales que deben estar acordadas en el contrato o en un documento de mutuo acuerdo sobre comprometer información delicada de la institución.

Figura 62. **Ejemplo de un contrato de confidencialidad**



CONTRATO DE CONFIDENCIALIDAD

CONTRATO DE CONFIDENCIALIDAD QUE CELEBRAN POR UNA PARTE _____. REPRESENTADA POR _____ Y POR LA OTRA PARTE D. _____ AL TENOR DE LAS DECLARACIONES Y CLAUSULAS SIGUIENTES:

DECLARACIONES

Declara la Empresa_____, por conducto de su representante:

- Que es una sociedad mercantil debidamente constituida, como consta en la escritura pública _____, otorgada ante D._____, Notario de _____.
- D. _____ vecino de_____ con Documeto de identidad _____ en representación de la mencionada empresa.

Que es su voluntad obligarse en los términos de éste contrato.

Declara el Comprador, por medio de:

- D. _____ vecino de_____ con con Documeto de identidad._____ en representación propia.
- Que es su voluntad obligarse en los términos de éste contrato.

Declaran las partes, pro conducto de sus representantes:

1. Que han decidido transmitirse mutuamente cierta información confidencial, propiedad de cada una de ellas, relacionada con tecnologías, planes de negocios internos, y otros tipos, a la que en lo sucesivo se le denominará "Información Confidencial", relativa a la venta de una de las partes de los servicios de _____
2. Que cualquiera de ellas, en virtud de la naturaleza de éste contrato, podrá constituirse como parte receptora o parte divulgante.
3. Que se reconocen mutuamente la personalidad con la que comparecen a celebrar el presente convenio y manifiestan su libre voluntad para obligarse en los términos de las siguientes:

CLAUSULAS

PRIMERA. Las partes se obligan a no divulgar a terceras partes, la "Información Confidencial", que reciban de la otra, y a darle a dicha información el mismo tratamiento que le darían a la información confidencial de su propiedad.

Para efectos del presente convenio "Información Confidencial" comprende toda la información divulgada por cualesquiera de las partes ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible y que se encuentre claramente marcada como tal al ser entregada a la parte receptora.

SEGUNDA. La parte receptora se obliga a mantener de manera confidencial la "Información Confidencial" que reciba de la parte divulgante y a no darla a una tercera parte diferente de sus abogados y asesores que tengan la necesidad de conocer dicha información para los propósitos autorizados en la Cláusula Sexta de éste convenio, y quienes deberán estar de acuerdo en mantener de manera confidencial dicha información.

Fuente: Modelocontrato.net, modelo para un contrato de confidencialidad. http://bit.ly/K9eJid. Consulta: junio de 2015.

4.4.2.2. Integridad de la información

La integridad se refiere a que la información debe mantenerse libre de ser modificada sin autorización, es decir, mantener la información como fue generada y que no se preste a que alguien pueda modificarla ni mucho menos eliminarla si no está autorizada, si está dentro de sus atribuciones y si cumple con un procedimiento establecido y debidamente documentado, así como, tener un registro de los cambios que efectúe.

4.4.2.3. Disponibilidad de la información

La información debe estar disponible para los usuarios que tengan los permisos y el acceso debidamente justificado de acuerdo a sus atribuciones, su perfil laboral y además debe acceder a la información de acuerdo a un procedimiento documentado, no importando si se trata de información en bruto (archivos, carpetas, volcado de información desde bases de datos) o bien informes digitales, escritos y toda clase de información preprocesada que pueda ser blanco de ataques externos sobre la información a través de robos, manipulaciones, deterioro e incluso la eliminación o pérdida de la misma.

4.4.3. Enfoques de protección

La protección de la información de la institución debe tener prioridad en cualquier política de seguridad que se plantee, tomando en cuenta los diferentes tipos de información, su relevancia, ubicación, el costo de su mantenimiento, tratamiento y almacenamiento, pero por sobre todo se deben tener planes que contemplen la mayor cantidad de puntos débiles por donde puede romperse la cadena de seguridad.

Con base en la premisa de que una cadena se rompe por el eslabón más débil, entonces se debe poner énfasis y presupuestar la inversión sobre procedimientos, equipos, personal e infraestructura que permita fortalecer dichos puntos.

4.4.3.1. Vulnerabilidades

Las vulnerabilidades de los sistemas instalados deben identificarse con base al análisis por parte de los técnicos y profesionales involucrados en los procesos que puedan ser blanco de ataques sobre la información.

Para realizar una correcta identificación de vulnerabilidades, se deben utilizar herramientas tales como listas de verificación y software que identifican puntos vulnerables a nivel del sistema operativo y del cortafuegos o *firewall*:

Seguridad física:

- Monitorización ambiental
- Control de acceso
- Desastres naturales
- Control de incendios
- Inundaciones

Seguridad en las conexiones a Internet:

- Políticas en el *firewall*
- VPN
- Detección de intrusos

Seguridad en la infraestructura de comunicaciones:

- Control y administración de *routers*

Figura 63. ***Routers* o ruteadores**

Fuente: Tecnoshot, configuración de ruteadores. http://bit.ly/IxiJvm. Consulta: junio de 2015.

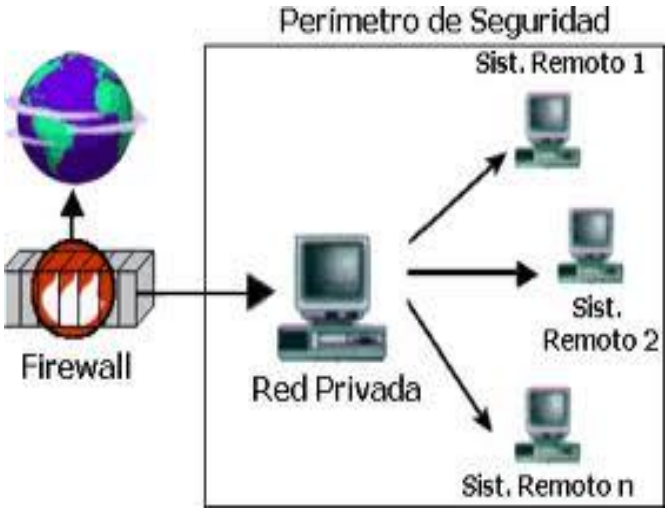
- Control, inspección física y lógica de *switches*

Figura 64. ***Switches***

Fuente: http://bit.ly/Ixj3Kq. Consulta: junio de 2015.

- Constante evaluación sobre las políticas de seguridad y reglas definidas en el *firewall*.

Figura 65. ***Firewall* o cortafuegos**



Fuente: SeguInfo, *firewalls* o cortafuegos. http://bit.ly/IxjeWg. Consulta: junio de 2015.

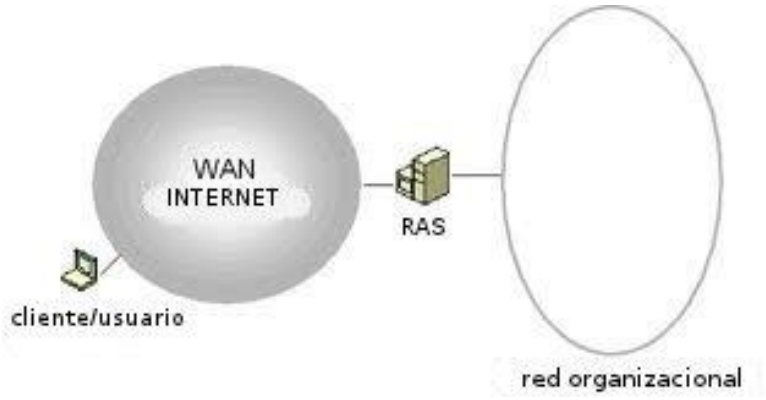
- Inspección y control de *hubs*, para evitar conexiones indeseadas o que no estén documentadas:

Figura 66. ***Hub* o concentrador**

Fuente: Jhonshos tecnología, *Hubs* y *switches*. http://bit.ly/IxjmoF. Consulta: junio de 2015.

- Los accesos remotos por medio de RAS, deben estar debidamente identificados y documentar su propósito, así como, establecer los responsables de dichas conexiones.

Figura 67. **RAS (*Remote Access Services*) Servicios de Acceso Remoto**



Fuente: eHow, Servicios de acceso remoto. http://bit.ly/1OkU7YP. Consulta: junio de 2015.

- Seguridad en Sistemas Operativos, que es de suma importancia debido a que el área de software es una de las más vulnerables debido a ataques por virus o intrusiones externas.

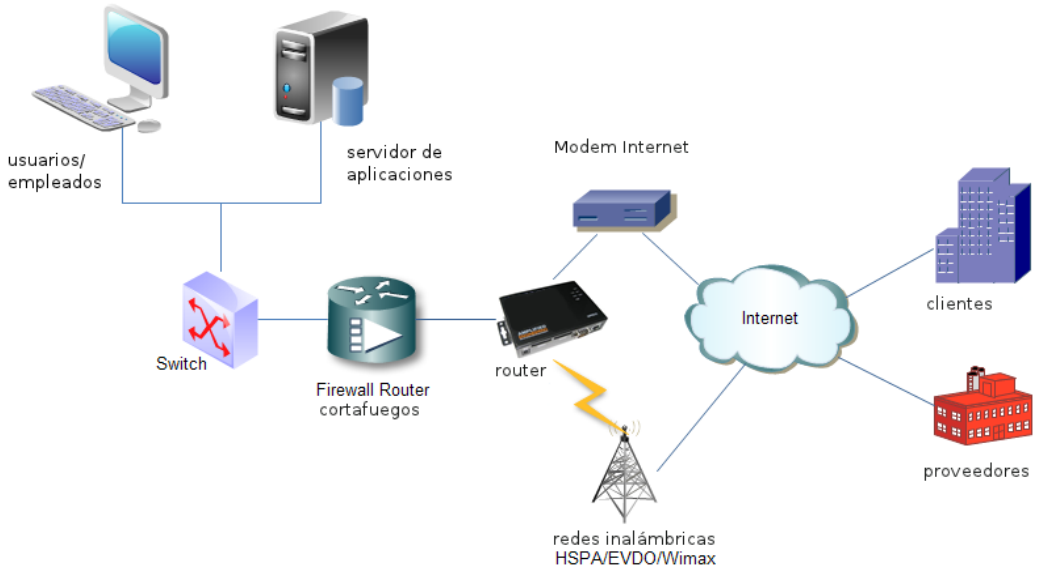
- Correo electrónico, es un medio muy vulnerable debido a que por medio de los archivos que se adjuntan, pueden enviarse códigos maliciosos, espías electrónicos, virus, entre otros.

- Seguridad en las aplicaciones críticas, debido a que la información más importante es la que se relaciona con el propósito de la institución, para este caso, se hace referencia a datos de empleados, estudiantes, catedráticos, proveedores, bancos del sistema, otras instituciones estatales vinculadas con la Universidad y por supuesto las mismas autoridades que de una u otra manera terminan en una o varias de las clasificaciones anteriores.

Para las aplicaciones más delicadas y que manejan información trascendente para la institución se deberá obtener una matriz de riesgo. Es muy importante que el software esté soportado por:

Sistema Operativo, servidores, redes de área local LAN, de área extensa WAN así como también el centro de cómputo.

Figura 68. **Infraestructura básica de una red con acceso a internet**



Fuente: elaboración propia.

También, con el fin de realizar una correspondencia con los datos obtenidos por medio de las listas de verificación, se debe contar con el uso de una herramienta especializada, la cual debe identificar vulnerabilidades en los Sistemas Operativos, ayudando de esta forma en el proceso de identificación de estas.

4.4.3.2. Amenazas

Cuando un proceso puede sufrir un ataque y este se puede identificar como una debilidad, se puede decir que está bajo amenaza, por lo tanto, las amenazas deben tenerse muy en cuenta, porque a pesar que una amenaza sólo es una probabilidad de ocurrencia no importando si es alta o baja, ésta puede ocurrir y causar daños.

Tabla III. **Niveles de probabilidad de amenazas**

Nivel		Definición
1	Alto	La amenaza tiene suficientes fundamentos y es altamente probable que ocurra.
2	Medio-alto	La amenaza está fundamentada y tiene buenas probabilidades de ocurrir.
3	Medio	La amenaza es posible que ocurra.
4	Medio-bajo	La amenaza tiene poca probabilidad de ocurrir.
5	Bajo	La amenaza no posee suficientes fundamentos y es muy poco probable que ocurra.

Fuente: elaboración propia.

4.5. Efectividad de las operaciones de contingencia

Las operaciones de contingencia son las respuestas y su velocidad de acuerdo al plan basado en la política de seguridad de información, estas operaciones incluyen las notificaciones sobre incidentes, así como, el proceso para recuperación de la operatividad luego de un ataque deliberado, un siniestro o algún accidente ya sea por causas voluntarias o involuntarias.

Recomendaciones:

- Contar con servicios de consultoría o soporte, previos a la implantación de cualquier herramienta asociada a esta categoría.

- Utilizar productos y herramientas para copias de seguridad como medida básica y fundamental de seguridad.

- Se debe considerar tener un centro de respaldo para garantizar la continuidad del negocio en caso de desastre. De preferencia este centro de respaldo debe estar físicamente fuera de la institución o por lo menos fuera del edificio en cuestión, con recursos propios o bien se puede contratar una empresa que preste ese servicio.

Escenarios de uso:

- Son de uso recomendado en cualquier tipo de organización cuyos procesos de negocio dependan del uso de sistemas de información.

- Son productos que pueden ser utilizados en organizaciones y empresas de cualquier tamaño.

- Son muy recomendables para la recuperación de la información y disponer de copias de seguridad.

Ámbitos de aplicación:

- Seguridad en aplicaciones y datos
- Seguridad en la red
- Seguridad en los sistemas
- Seguridad en el puesto de trabajo

4.5.1. Notificaciones y activaciones

Cuando un incidente de seguridad ocurre, la forma más rápida de hacerla del conocimiento de los principales involucrados en la política de seguridad o bien directamente al equipo de seguridad designado, de ser posible, es un sistema automatizado que envíe alertas ya sea por correo o a través de un software destinado a ese propósito, para que sea lo más rápidamente posible la notificación del incidente, para luego entrar a la fase de activación que es la puesta en marcha de las medidas necesarias de recuperación de acuerdo a los planes elaborados previamente sobre contingencias.

Figura 69. **Gestión de incidentes de seguridad de información**

Fuente: Instituto nacional de ciberseguridad, España. Gestión de seguridad informática. http://bit.ly/1U1Apmp. Consulta: junio de 2015.

4.5.2. Reanudación de operaciones

Teniendo en cuenta que luego de un incidente de seguridad de información, la institución debe recuperar el ritmo normal de trabajo que tenía antes de un desastre o un ataque premeditado. Se debe tomar en cuenta que se tiene que asegurar que los recursos disponibles se van a utilizar para recuperar las funciones y actividades normales tras una emergencia o desastre que haya afectado a la institución.

Se deben tener establecidos los procedimientos que se deben ejecutar inmediatamente después de un incidente para restablecer las actividades y procesos principales lo antes posible y con el menor impacto sobre las actividades, los empleados, los clientes externos e internos, los proveedores y demás involucrados en los procesos en cuestión.

4.5.3. Recuperación

La recuperación, luego de un desastre, debe realizarse a la brevedad posible y esta incluye los datos, los equipos y el software crítico que fue dañado o que se inutilizó durante el desastre o ataque a los equipos o directamente a la información. Este procedimiento es crucial luego de un incidente de seguridad porque el tiempo que se tarda la institución en recuperarse de un desastre, significa atrasos y pérdidas que van desde equipos, información, despidos de personal e incluso la pérdida de confianza en los clientes internos y externos.

Por ello, es importante que el proceso de recuperación esté bien documentado y sea del conocimiento de los colaboradores del departamento, así como su utilización y puesta en marcha, los alcances y límites en función del tiempo, recursos y esfuerzo que se deben dedicar a este tipo de eventos y sobre todo la concientización de los empleados para enfrentar situaciones cruciales que comprometan el desempeño normal de las actividades, para que la recuperación sea lo menos complicada posible y que las pérdidas se minimicen o en el mejor de los casos sean nulas y en un tiempo prudencial que ya esté contemplado en los documentos del plan, la empresa esté de regreso a sus actividades normales y funcionando como hasta antes del incidente ocurrido.

En un sistema de gestión de incidentes de seguridad de información es importante considerar un Plan de Recuperación ante Desastres (DRP por sus siglas en inglés), el cual tiene diferentes maneras de abordarlo, pero éste siempre debe estar alineado con el plan de continuidad, por lo que debe considerar los elementos que definen la razón de ser de una organización.

El Plan de Recuperación ante Desastres debe incluir los criterios para determinar cuándo un incidente de seguridad no se puede resolver mediante los procedimientos comunes de atención y se considera como un desastre, es decir, cuando se presenta un evento catastrófico y repentino que anula la capacidad de las organizaciones para llevar a cabo los procesos esenciales.

Un desastre podría ser el resultado de un daño importante a una parte de las operaciones, la pérdida total de una instalación o la incapacidad de los empleados para acceder a las instalaciones, generado por algún tipo de desastre natural, una contingencia sanitaria o una huelga, por ejemplo.

Una propuesta para el desarrollo y aplicación del DRP se considera en los siguientes 6 puntos:

1. Desarrollar una política de continuidad del negocio

   Todas las actividades deben estar alineadas con los objetivos de continuidad del negocio, por lo que un punto de partida puede ser el desarrollo de una política encargada de establecer el marco de operación de los planes, así como la clasificación de los sistemas o aplicaciones para identificar aquellos que sean considerados como críticos.

2. Realizar una evaluación de riesgos

   Llevar a cabo una evaluación de riesgos permite identificar, analizar y evaluar las amenazas que podrían afectar a la organización, especialmente aquellos que puedan provocar un evento que se incluya en la categoría de desastre.

3. Realizar un análisis de impacto al negocio (BIA)

En este paso se definen principalmente los objetivos de recuperación para los sistemas que soportan los procesos de negocio. Se define el Tiempo Objetivo de Recuperación (RTO por sus siglas en inglés), que es el período permitido para la recuperación de una función o recurso de negocio a un nivel aceptable luego de un desastre, y el Punto Objetivo de Recuperación (RPO) que describe la antigüedad máxima de los datos para su restauración, con base en los requisitos del negocio.

4. Desarrollar estrategias de recuperación y continuidad del negocio

En este paso se busca dejar en claro todas las medidas a poner en práctica para regresar a la operación tan pronto como sea posible, con base en una priorización derivada de la clasificación del primer punto.

5. Concientizar, capacitar y probar los planes

Un elemento necesario con relación a los planes consiste en realizar su difusión entre los miembros de la organización, especialmente entre aquellos que serán los encargados de ponerlo en ejecución en caso de ser requerido. Además, es necesario que se lleven a cabo pruebas del mismo, para ello, se puede hacer uso de diferentes opciones, desde una revisión de la lista de verificación (*checklist*) de la recuperación hasta una prueba de interrupción completa (*full interruption test*) donde las operaciones se interrumpen en el sitio primario y se transfieren a un sitio de recuperación.

6. Mantener y mejorar el plan de recuperación ante desastres

A partir de los resultados de la prueba de los planes se deben llevar los ajustes correspondientes para contar con documentación actualizada y apropiada a los intereses de la organización, una vez que han sido consideradas las situaciones de desastre que podrían afectarla, las actividades y recursos necesarias para restablecer las operaciones críticas.

5. SEGUIMIENTO O MEJORA CONTINUA

5.1. Resultados

Los resultados sobre un análisis de seguimiento para una política de seguridad de información deben estar claramente medidos y expresados en cantidades relativas a un indicador. Los indicadores para un proceso de evaluación y mejora continua deben estar previamente definidos, porque de ellos dependerá mucho el análisis de los resultados obtenidos en mediciones realizadas cuando la política esté en marcha.

Como premisa, en esta fase de la política se debe tomar en cuenta lo expuesto por Herrera Reyna: “No se puede evaluar lo que no se puede medir y para poder medir un proceso se debe contar con algún tipo de indicadores.” [3]

Para tener cubiertas las áreas más importantes de la institución con respecto a los indicadores que se deben definir, se pueden destacar las que son fundamentales, dichas áreas son:

- Herramientas lógicas de seguridad
- Buenas prácticas
- Políticas y planes

[3] HERRERA REYNA, Omar Alejandro. http://candadodigital.blogspot.com/ .[Consulta: mayo de 2015].

- Seguridad global
- Confianza en los sistemas
- Malware
- Equipos en riesgo

Figura 70. **Ejemplo de indicadores de seguridad de información**

Nombre del Indicador	Formula del Indicador	Estado Inicial	Valor Esperado	Periodo
% de acciones implementadas	(# de acciones implementadas/ total de acciones) * 100	0% no se había hecho antes implementación de la norma ISO 27001	100% logrado de implementar las acciones de la norma	4 meses
% de equipos actualizados	(# de equipos actualizados/ total de equipos) * 100	Se inicia con un 50% de los equipos actualizados	100% de los equipos actualizados e instalados	4 meses
% de fallas corregidas	(# fallas corregidas/ total fallas detectadas) * 100	0% no se había hecho esta medición antes	100% de las fallas importantes sean corregidas	4 meses
% de personas capacitadas	(# personas que asisten a capacitación/ total de personas a capacitar) *100	0% no se había realizado estas capacitaciones nunca antes	100% de las personas de la organización estén capacitadas	4 meses
Calificación promedio de la evaluación	Suma de calificación de las evaluaciones/ # personas evaluadas	0 porque es la primera evaluación que se va a realizar	4 puntos en una escala de 1 a 5 siendo 1 muy malo y 5 excelente	4 meses
% detecciones documentadas	(# detecciones documentadas/ total detecciones) * 100	0% no se había realizado reporte de detecciones ni su documentación	100% de detecciones documentadas	4 meses

Fuente: SlideShare, indicadores de seguridad de la información. http://bit.ly/1LvZenD. Consulta: junio de 2015.

Para definir correctamente los indicadores será necesario un esfuerzo conjunto porque de ello dependerá las medidas y contramedidas que se tomen respecto a las amenazas e incidentes de seguridad, debido a que los indicadores se deben definir con base al criterio de que, las variables a ser analizadas, puedan ser medidas y evaluadas, para luego realizar un análisis con suficiente información, para que se puedan tomar medidas correctivas respecto a la seguridad de los sistemas de información.

5.1.1. Indicadores

No se puede evaluar lo que no se puede medir, y para poder medir un proceso se debe contar con algún tipo de indicadores.

Los KPI ("*key performance indicators*", o indicadores claves del desempeño) son métricas orientadas a cuantificar el grado de cumplimiento para un objetivo de negocio, por parte de un proceso.

Casi en cualquier disciplina moderna, especialmente las que tienen que ver con tecnología, se debe tener considerado el uso de KPI. Esto debido a que si, por ejemplo, los clientes nos exigen resultados tangibles, no es suficiente con que se tenga la idea de que se están haciendo bien las cosas, si no existen pruebas contundentes a través de números que indiquen con certeza cómo y de qué manera se están alcanzando los objetivos y metas propuestas, entonces tenemos una clara señal de que no se están definiendo bien los indicadores, las métricas y por lo tanto los KPI no están ayudando o bien están midiendo datos que no interesan.

La mayoría de las métricas que se utilizan en seguridad de información, desafortunadamente no cumplen con esta definición. Normalmente, usamos indicadores de efectividad técnica u operativa, los cuales no podemos relacionar directamente con el cumplimiento de objetivos o las políticas de la institución. Además, la mayoría de estos indicadores son específicos para cada control (no describen un proceso, que es otro requerimiento para considerar como clave a un indicador).

Algunos ejemplos de indicadores que usamos típicamente en seguridad:

- Número de ataques prevenidos/detectados.
- Número de programas maliciosos detectados (virus, *spyware*, troyanos, *malware*, etcétera.).
- Número de incidentes de seguridad reportados y atendidos (equipos de respuesta ante incidentes).
- Número de actualizaciones de seguridad.
- Tiempo de respuesta para atender incidentes.
- Tiempo promedio de distribución de parches de seguridad.
- Tiempo promedio de restauración de un sistema a partir de un incidente
- Tiempo de respuesta promedio para solución de un incidente

Los datos obtenidos a partir de mediciones, encuestas, estadísticas, incidentes ocurridos y toda la información que pueda ser sujeta a análisis, se deberá clasificar en cualitativa y cuantitativa.

La información cualitativa deberá ser cuantificada para que pueda ser objeto de análisis, porque la información de este tipo, por su naturaleza, no tiene una forma básica para medirse, por lo tanto, deben construirse tabulaciones de dicha información que permitan su homologación numérica, es decir, se deben definir grados o ponderaciones del atributo o cualidad y su correspondiente valor numérico.

Para la información cuantitativa, se debe tomar en cuenta que proviene de diferentes medidas y por lo tanto, de diferentes escalas que dificultan una comparación simple entre ellas. Una de las maneras de hacerlas comparables es: clasificar la información de cada indicador en tablas que muestren los grados ponderados de cada característica. Esta escala se debe crear con valores mínimo, máximo e intermedios que logren agrupar todo el rango de valores del indicador cuantitativo.

5.1.2. Análisis

El análisis debe estar orientado a poder probar las hipótesis planteadas en relación a los datos obtenidos en etapas de captura de datos por incidentes, ya sea datos históricos que nos pueden dar una mejor medida para realizar pronósticos.

El análisis de riesgos en seguridad de información es un procedimiento utilizado para determinar el riesgo asociado a los activos de cómputo relacionados y la pérdida debido a la manifestación de las amenazas. El procedimiento de análisis de riesgos primero determina el nivel de vulnerabilidad del activo tras identificar y evaluar el efecto de los elementos de control situados en cada lugar o momento del procedimiento establecido. Los niveles de vulnerabilidad para un activo y en relación a una determinada amenaza, se determina con controles que se deben situar en cada lugar al momento en que se realiza el análisis de riesgo.

Figura 71. **Reducción de riesgo**

Fuente: ERB, Marcus. Gestión de riesgo en la seguridad informática. http://bit.ly/1TXewXU. Consulta: agosto de 2015.

Un análisis de riesgos de seguridad define el ambiente actual y realiza las acciones correctivas recomendadas si el riesgo residual no es aceptable. Esto se debe considerar como una parte esencial de un programa de manejo de riesgos en seguridad de información. El proceso de análisis de riesgo debe ser realizado con regularidad suficiente para asegurar que las aproximaciones del manejo del riesgo de la organización correspondan a una respuesta real acorde los riesgos actuales asociados con la información de los activos. El manejo de riesgos debe indicar si acepta el riesgo residual o implementa las actividades recomendadas.

El objetivo del análisis de riesgos es poder tener la capacidad de:

- Identificar, evaluar y manejar los riesgos de seguridad.
- Estimar la exposición de un recurso a una amenaza determinada.
- Determinar qué combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable.
- Tomar mejores decisiones inmediatamente después de un incidente de seguridad de la información.
- Enfocar recursos y esfuerzos en la protección de activos.

5.1.3. Interpretación

Los datos recabados deben ser separados, clasificados o categorizados, de tal manera que de todo el análisis numérico y estadístico realizado se pueda convertir en una correcta interpretación de los índices, porcentajes, gráficas y todos los modelos que se construyeron durante el análisis de la información que en esta fase muestra los patrones y tendencias en los datos que se pretendía obtener. Los datos analizados e interpretados pueden ser entonces usados como evidencia para argumentar científicamente y así corroborar una hipótesis o teoría.

Para el caso del análisis de información sobre incidentes de seguridad, lo más deseable sería que con base en la información obtenida, se pudiera llegar a interpretar la información de tal manera que arroje datos sobre los eventos que más han sucedido o que tienden a ser más comunes, los que por experiencias o datos externos presentan un grado de riesgo tentativo, para que luego esos resultados interpretados sean sometidos a una discusión entre los diferentes grupos que componen el departamento en relación a la seguridad de los datos.

Por ejemplo, si ocurre un incidente de seguridad grave, lo más importante para el manejo de dicho incidente puede iniciarse un proceso para paliar de manera directa el problema tomando en cuenta las siguientes recomendaciones:

- No ocultarlo. Lo mejor sería comunicar lo antes posible a los mandos medios y a la jefatura para poder iniciar una estrategia para paliar la crisis debido al incidente ocurrido.

- Mantener la calma por la situación e iniciar el proceso de recuento de daños, estimación de pérdidas, cuantificación de equipos, documentos, personas y procesos afectados, así como el grado de daños ocurridos.

- No iniciar buscando culpables. No se debe perder el tiempo buscando culpables, eso representa tiempo valioso para detener otros daños.

- Obtener información de primera mano y verificarla. La información de primera mano puede ser ofrecida por el personal que ha reportado el incidente o bien alguno de los miembros del equipo de seguridad de información designado. Se debe elaborar un informe técnico lo antes posible para poder tener un panorama general de los daños causados y para que se pueda diseñar una estrategia que inicie una recuperación de información y la reactivación de los procesos de producción que pudieran haber sido afectados por el incidente, tan pronto como sea posible.

- Establecer un plan de acción y coordinarlo. El plan de acción que se inicia a partir de la información brindada a partir del análisis situacional después de ocurrido un incidente, debe involucrar al jefe y a todos los empleados que tienen que ver con el proceso o los equipos afectados debido al incidente en cuestión ya que ellos son los que conocen detalles que pueden significar la pronta recuperación del proceso afectado.

Aparte de ello se debe coordinar y priorizar las tareas para los involucrados, anteponiéndolas a los planes de ejecución normales y declarar un estado de emergencia para que todos los esfuerzos se enfoquen en mitigar los daños y volver a las labores normales inmediatamente después de haber solucionado al menos los problemas más complejos que se hayan encontrado debido al incidente de seguridad.

5.1.4. Discusión

Luego del análisis debe hacerse una discusión para determinar el mejor camino a seguir. Esto se debe realizar entre los diferentes grupos nombrados por jefatura, los coordinadores de área, los responsables de aplicaciones, los auditores internos y todos los que se vean involucrados en el procesamiento de la información de la institución y los encargados de la infraestructura tecnológica.

Figura 72. **Gestión eficiente de incidentes de seguridad**

Fuente: elaboración propia.

Para que juntos puedan tomar decisiones sobre cada uno de los casos analizados y llegar a conclusiones en la línea de futuras inversiones sobre equipos, capacitaciones, nuevo software, contratación de más empleados de ser posible o la reorganización de las áreas, mejoras o cambios en la ubicación de equipos, sistemas de alimentación eléctrica, caídas de aguas pluviales, sistemas de alarmas e incendios, seguros, puertas de acceso, guardias, cajas de seguridad, sistemas de alta disponibilidad y sistemas para copias de seguridad internos o externos.

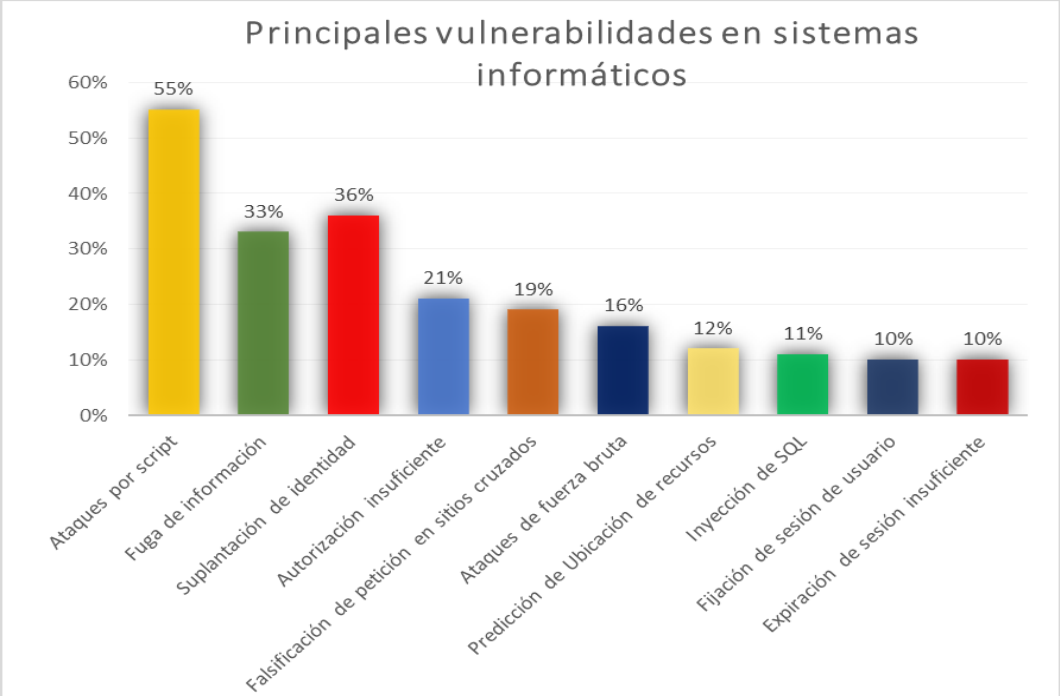
Aparte de ello, se deben realizar las revisiones a la documentación relacionada con los incidentes analizados, esto puede dar paso a modificar los anteriores manuales de operación, normativos, reglamentos y también una revisión y posible modificación a la política de seguridad, que de no hacerlo si se llega a conclusiones que así lo apunten, se correrá el riesgo de repetir incidentes de la misma manera que en el ciclo anterior o bien dar paso a incidentes aún más desastrosos.

5.2. Estadísticas

Las estadísticas son quizá el mejor aliado para determinar el grado de ocurrencia de los incidentes, así como, asignarles importancia debido a la frecuencia con que ocurren los ataques o incidentes de seguridad en la institución.

Se deben establecer métodos estadísticos ya sea a través de algún software para el análisis de información que ya está preprocesada para llegar a obtener resultados que puedan realimentar la política y su correcta aplicación en un ciclo de trabajo futuro.

Figura 73. **Porcentaje de vulnerabilidades en sitios de internet**



Fuente: elaboración propia, con base en datos de White Hack Security Website. Consulta. junio de 2015

5.3. Ventajas

El seguimiento tiene como principales ventajas la retroalimentación del sistema de recuperación sobre fallas o incidentes sobre la seguridad de información.

Figura 74. **Proceso de seguimiento control y evaluación**

Fuente: Sistema de seguimiento, control y evaluación. http://bit.ly/1Lw0ZBc. Consulta, junio de 2015.

Algunas de las ventajas puntuales que se pueden destacar son:

- Posibilita la identificación, tratamiento y solución de los problemas o el aprovechamiento de oportunidades.

- Permite eliminar o atenuar las debilidades y afianzar e incrementar las fortalezas.

- Analizar los procesos, renovar y actualizar los mismos, permitiéndole a la organización ser más competitivas, eficaz y eficiente.

- Obtener mejoras a corto plazo, no solo en la parte productiva o de servicio sino en la administrativa también.

- Aunque no es posible eliminar por completo los incidentes, posibilita su disminución, por lo que reduce los costos, para la organización.

- Permite el ajuste de los procesos con el desarrollo tecnológico, incrementando productividad.

5.4. Desventajas

Un plan de mejora continua se enfrentará con muchos problemas que serán en su mayoría tendientes a la cultura laboral, incluso desde los mandos superiores podrá existir una resistencia al cambio, falta de compromiso, constancia y disciplina que regularmente ocurre también en los mandos medios y empleados en general. Algunas de las desventajas puntuales que se pueden mencionar son:

- Puede ser difícil hacer cambiar los paradigmas de participación de los empleados para llevar a cabo un plan de seguridad.

- Para la obtención de resultados tangibles es necesario para que los cambios se realicen en toda la organización.

- En la mayoría de ocasiones es imprescindible hacer inversiones de consideración.

- Si no se observan las medidas adecuadas, con celeridad y oportunidad, el proceso se puede tornar muy largo para la consecución de los resultados deseados.

5.5. Relación beneficio/costo

La diferencia esencial entre el análisis de costo-beneficio para una institución pública (en este caso la Universidad de San Carlos de Guatemala) y los métodos ordinarios de evaluación de inversiones que emplean las empresas lucrativas, es el énfasis en los costos y beneficios sociales.

El objetivo consiste en identificar y medir las pérdidas y las ganancias en el bienestar económico que recibe la sociedad (en este caso, la población estudiantil, unidades académicas, dependencias de la universidad, empleados y público en general) en su conjunto.

Para realizar un análisis por separado tomando en cuenta las inversiones que se pretenden realizar en cuanto a seguridad de información, se puede elaborar una tabla con cada uno de los proyectos a implementar, por ejemplo: sistema contra incendios, cambio o remodelación del sistema de aire acondicionado en el cuarto de servidores, antivirus, *firewall*, sistema automatizado de copias de seguridad, entre otros.

Un método sencillo para calcular los beneficios y costos asociados a la inversión en seguridad es conocido como método ROSI, el cual es una variante del método ROI, que es un modelo de reducción de vulnerabilidades. El método ROSI se usa para justificar la inversión en seguridad de la información en términos monetarios, en donde la inversión es el costo de la implementación de medidas de seguridad y el retorno es la diferencia entre las pérdidas actuales por incidentes de seguridad y las pérdidas esperadas luego de aplicar dichas medidas de seguridad.

Tabla IV. **Tabla de análisis de costo-beneficio**

Proyecto (características)	Costo	Beneficio	Costo/Beneficio	Deseable [Si/No]

Fuente: elaboración propia.

Para realizar una estimación general sobre una implementación usando este método, se deben utilizar las siguientes ecuaciones:

$$ROSI = Retorno / Costo$$

Por lo tanto:

$$ROSI = (Valor – Costo) / Costo$$

Un ROSI aceptable debe ser positivo, es decir, cuando el valor es mayor que el costo.

5.6. Auditorías

Las auditorías siempre tendrán como principal objetivo hacer las observaciones sobre fallos en la continuidad de los sistemas para con ello determinarlas, luego corregirlas para mejorar la eficiencia de los mismos.

Una auditoría de seguridad consiste en apoyarse en un tercero de confianza (generalmente una compañía que es especializada en la seguridad informática) para validar las medidas de protección que se llevan a cabo, sobre la base de la política de seguridad.

Figura 75. **Auditorias y entorno seguro**

Fuente: Encrypted TBN2, auditorías. http://bit.ly/1HZ9T3d. Consulta, agosto de 2015.

Aunque pueden existir las auditorías propias o internas que brindan un diagnóstico que puede servir de mucho para darle seguimiento a los problemas que se detecten.

El objetivo de la auditoría es verificar que cada regla de la política de seguridad se aplique correctamente y que todas las medidas tomadas conformen un todo coherente.

Una auditoría de seguridad garantiza que el conjunto de disposiciones tomadas por la empresa se consideren seguras.

Para cumplir con estándares internacionales, la institución puede basarse en ISO/IEC 27001, que es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad, sector público y tecnologías de la información.

También es muy eficaz para organizaciones que gestionan la información por encargo de otros, por ejemplo, empresas de subcontratación de personal en áreas tecnológicas. Puede utilizarse para garantizar a los clientes que su información está protegida.

Un servicio de auditoría para seguridad de información consta de las siguientes fases:

- Enumeración de redes, topologías y protocolos.
- Verificación del Cumplimiento de los estándares internacionales. ISO, COBIT, etc.
- Identificación de los sistemas operativos instalados.
- Análisis de servicios y aplicaciones.
- Detección, comprobación y evaluación de vulnerabilidades.
- Medidas específicas de corrección.
- Recomendaciones sobre implantación de medidas preventivas.

5.6.1. Auditorías internas

El programa de auditorías internas se propone anualmente. En su elaboración se toma en consideración tanto el estado y la importancia de los procesos ejecutados, como los resultados de auditorías previas.

Para la ejecución de las auditorías internas, se deberá disponer de un equipo de personas debidamente calificadas y nombradas por la jefatura. La existencia de este conjunto de auditores garantiza la objetividad e imparcialidad del proceso de auditoría, evitando de esa manera que los auditores auditen su propio trabajo.

El delegado de las auditorías internas o bien el equipo mismo, se asegura de que se realizarán todas las acciones para eliminar las no conformidades detectadas y sus causas.

Las acciones correctivas que surjan como consecuencia de la auditoría y su plazo de implantación, serán documentadas y puestas en práctica por el personal afectado, de acuerdo a lo establecido en la política de seguridad.

Las actividades obligatorias de seguimiento a las auditorías internas, incluyen la verificación de las acciones tomadas y el informe de los resultados de tal verificación.

5.6.2. Auditorías externas

Durante una auditoría externa se realizan inspecciones sobre los procesos y sistemas de información, para evaluar el estado de la seguridad física, la seguridad de los procedimientos, la seguridad de los sistemas de información, la capacidad de destrucción y recuperación de la información y asegurar que esta sea evaluada y protegida contra toda forma de acceso, uso, divulgación, modificación, destrucción y garantizar la confidencialidad, integridad, disponibilidad y autenticación.

También analiza el flujo de información para determinar cuáles son los principales riesgos y los impactos que generaría en el negocio la ocurrencia de ataques contra la integridad, disponibilidad de datos y confidencialidad de estos, cómo repercutiría en el prestigio de la institución y cómo se repondría de los daños ocasionados.

5.6.3. Auditorías de certificación

La certificación del sistema de gestión de seguridad de información, es el proceso mediante el cual una empresa u organismos avalados por la ISO, externa a la organización, verifica el cumplimiento de las condiciones o normativas de las ISO 27001:2005 certificable. La certificación no es de carácter obligatoria, ya que es la empresa o institución, quien decide solicitar la certificación ante dichos organismos. Existen muchas razones para que las empresas decidan certificarse, entre esas podemos relacionar las siguientes:

- Conservar la confianza de sus clientes y aumentarlos.
- Posicionar el buen nombre de la empresa ante el mercado.
- Aumentar su competitividad

- Crear disciplina y compromiso de los empleados de la empresa entorno a la seguridad de la información.

Pero todo lo anterior no puede ser posible si la institución no tiene instauradas y en normal funcionamiento las políticas de seguridad de información basadas en la Norma ISO 27001:2005, lo cual es un paso ulterior a la definición de un plan de políticas de seguridad de información.

CONCLUSIONES

1. La política de seguridad de información debe divulgarse y ponerse a disposición de todos los involucrados en los procesos de aseguramiento de información que deben estar definidos en la política de seguridad, así como, clientes internos y externos que puedan tener alguna participación ya sea en accesos a las aplicaciones, a los servidores, a redes públicas y privadas, así como, a equipo que pueda ser objeto de ataques que comprometan la información que se resguarda.

2. Los riesgos son latentes y no existen sistemas perfectos de seguridad, así que lo más importante es lograr identificar y delimitar los riesgos a que está sometida la información, así como, los procedimientos en caso se conviertan en incidentes lamentables, para lograr con ello, una mejor reacción de parte de los equipos designados para incidentes de esa naturaleza.

3. Los controles definidos en la política de seguridad deben ir acorde a los riesgos identificados en los análisis previos y para ello se debe estar consciente que es necesario en la mayoría de casos, realizar inversiones que muchas veces son cuantiosas pero que a la larga darán mayor tranquilidad a la institución en cuanto a la información que se administra.

4. Los estándares y procedimientos que se definan en la política de seguridad de información deben estar acorde a los tiempos que se viven, es decir, basados en técnicas modernas, con instrumentos actualizados, tales como métodos recientes, software moderno y actualizado, personal capacitado y sobre todo que los procedimientos estén sujetos a revisión periódica para ser actualizados de ser necesario.

5. En cuanto a la implementación de la política, debe ser un mandato y no una sugerencia de parte de la gerencia y debe aplicarse a todo el personal involucrado directa o indirectamente, sin excepciones.

6. Todos los empleados que tengan a su cargo algún procedimiento o equipo que administre, almacene o procese información, deberá tener un rol y permisos definidos con base a la política de seguridad de información y a su perfil laboral. Estos permisos y roles deberán ser intransferibles y bajo ninguna circunstancia se compartirán entre los empleados. Esto logrará una mejor administración de las responsabilidades.

7. El seguimiento y continuidad de la política de seguridad de información deberá ser establecido, puesto a la vista y divulgarse a la brevedad posible para que todos los empleados estén enterados del mismo para que así comprendan y acaten las disposiciones contenidos en dichos documentos.

RECOMENDACIONES

1. La implementación de la política de seguridad de información debe llegar en un plazo no muy largo, a convertirse en parte de la cultura organizacional en la institución. Idealmente, todos los empleados involucrados deben formar parte de los equipos designados por la gerencia para hacer frente a los desafíos que representa el mantener un sistema de aseguramiento de la información y lograr con ello en un mediano plazo, iniciar el camino hacia una certificación internacional y la futura implementación de un sistema de gestión de seguridad de información basado en estándares internacionales por ejemplo bajo la Norma ISO/IEC 27001:2005.

   Lo cual brindará garantías a los clientes internos y externos de que la información que confían está resguardada bajo normas y procedimientos de calidad internacional, mostrando así una mayor madurez como institución, también haciendo notar el compromiso de la gerencia hacia el tratamiento de la información, así como, brindar mejores productos y servicios en el área tecnológica.

2. Es preciso encaminar los esfuerzos de todo el personal para lograr que las políticas de seguridad de información se conviertan en una certificación de calidad mundial y no caer en los mitos de que los estándares de calidad son solamente para empresas grandes.

Es un error pensar de esa manera porque cualquier empresa puede lograr la certificación de la calidad de sus productos o servicios, lo cual le dará un valor agregado frente a la competencia y así podrá enfrentar de mejor manera el gran desafío que significa resguardar información y sobre todo hacerlo con responsabilidad y fiabilidad.

BIBLIOGRAFÍA

1. Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento AGESIC. *Política de gestión de incidentes de Seguridad de la Información* [en línea]. Montevideo, Uruguay. Disponible en versión PDF: http://goo.gl/z1Jm3. [Consulta: 8 de marzo de 2011].

2. ALEXANDER, Alberto G. *Diseño de un sistema de gestión de seguridad de información: óptica ISO 27001:2005.* Colombia: Alfaomega, 2007. 176 p. ISBN: 9789586827133.

3. BORGHELLO, Cristian Fabián. *Seguridad informática sus implicancias e implementación.* Trabajo de graduación de Ing. Informática. El Salvador. Universidad Francisco Gavidia, Facultad de Ingeniería. 2001. 309 p.

4. Gestiópolis. *Mejoramiento continuo y Kaizen* [en línea] México. http://goo.gl/axrgj. [Consulta: 17 de agosto de 2011].

5. GÓMEZ VIEITES, Álvaro. *Enciclopedia de la seguridad informática.* España: Editorial RA-MA, 2006. 696 p. ISBN:9788478977314.

6. Instituto ROI (Return On Investment). *¿A qué nos referimos cuando hablamos de usar el ROI para Evaluar?* [en línea] Santiago, Chile. Disponible en versión PDF: http://goo.gl/9lMER. [Consulta: 10 de mayo de 2012].

7. International Organization for Standardization. *Código de buenas prácticas en la gestión de la seguridad de la información.* Norma Estándar ISO/IEC Internacional 17799/UNE 71502. Ginebra,Suiza: ISO. 2005.

8. MATALOBOS, Juan Manuel. *Análisis de riesgos de seguridad de la información.* Trabajo de graduación de Ing. Informática, Universidad politécnica de Madrid, Facultad de Informática. España. 2009. 274 p.

9. ORMELLA, Carlos. *ROSI, Retorno sobre la inversión de seguridad* [en línea]. Argentina: AltoSec Blog. Disponible en versión PDF: http://goo.gl/O7ziq. [Consulta: 20 de enero de 2012].

10. RAMIÓ, Jorge. *Seguridad Informática y Criptografía* [en línea]. Versión 4.1. [Madrid, España]: Universidad Politécnica de Madrid. Disponible en versión PDF: http://goo.gl/ovsku. [Consulta: 3 de abril de 2012].

ANEXO

Anexo 1. **Modelo para un contrato de confidencialidad**

Acuerdo de Confidencialidad

Entre los suscritos a saber, por una parte _____, *mayor de edad* y domiciliado(a) en la ciudad de _____, identificado(a) como aparece *al pie de su respectiva firma*; y por la otra, _____, también mayor de edad y domiciliado en la ciudad de _____, identificado(a) como aparece al pie de su firma , quien actúa en nombre de _____, se ha acordado celebrar el presente Acuerdo de Confidencialidad que se regirá por las siguientes cláusulas, previas las siguientes

CONSIDERACIONES

1. Las partes están interesadas en: _____

2. Debido a la naturaleza del trabajo, se hace necesario que éstas manejen información confidencial y/o información sujeta a derechos de propiedad intelectual, antes, durante y en la etapa posterior.

CLÁUSULAS

PRIMERA. OBJETO. El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre ellas, incluyendo información objeto de derecho de autor, patentes, técnicas, modelos, invenciones, *know-how,* procesos, algoritmos, programas, ejecutables, investigaciones, detalles de diseño, información financiera, lista de clientes, inversionistas, empleados, relaciones de negocios y contractuales, pronósticos de negocios, planes de mercadeo e cualquier información revelada sobre terceras personas.

SEGUNDA. CONFIDENCIALIDAD. Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el transcurso de _____,

será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizado previamente por la parte de cuya información confidencial se trata. Se considera también información confidencial: a) Aquella que como conjunto o por la configuración o estructuración exacta de sus componentes, no sea generalmente conocida entre los expertos en los campos correspondientes. b) La que no sea de fácil acceso, y c) Aquella información que no este sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial.

TERCERA. EXCEPCIONES. No habrá deber alguno de confidencialidad en los siguientes casos: a) Cuando la parte receptora tenga evidencia de que conoce previamente la información recibida; b) Cuando la información recibida sea de dominio público y, c) Cuando la información deje de ser confidencial por ser revelada por el propietario.

CUARTA. **DURACION.** Este acuerdo regirá durante el tiempo que dure _____ hasta un término de tres años contados a partir de su fecha.

QUINTA. **DERECHOS DE PROPIEDAD.** Toda información intercambiada es de propiedad exclusiva de la parte de donde proceda. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso.

SEXTA. **MODIFICACIÓN O TERMINACIÓN**. Este acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de ambas partes.

SÉPTIMA. **VALIDEZ Y PERFECCIONAMIENTO.** El presente Acuerdo requiere para su validez y perfeccionamiento la firma de las partes.

Para constancia, y en señal de aceptación, se firma el presente acuerdo en ___ ejemplares, por las partes que en él han intervenido, en la ciudad de _____ a los _____ (__) días del mes de _____ de _____ (201_).

_____	_____
Firma	Firma
_____	_____
Documento de Identidad	Documento de Identidad

Fuente: I-Uris.com, Derecho de internet en Colombia. http://bit.ly/1L0Acy8. Consulta: 15 de mayo de 2012.