

**UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA**



**FACULTAD DE INGENIERÍA DE SISTEMAS E  
INFORMÁTICA**



**“Seguridad en Aplicaciones Informáticas”**

**INFORME DE TRABAJO PRÁCTICO DE SUFICIENCIA**

**PARA OPTAR EL TÍTULO DE:  
INGENIERO DE SISTEMAS E INFORMÁTICA**

**PRESENTADO POR EL BACHILLER:  
JUANITO AMASIFUEN SHUPINGAHUA**

**ASESOR:  
ING. RAFAEL VILCA BARBARAN**

**IQUITOS – PERÚ  
2015**

**UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA**



**FACULTAD DE INGENIERÍA DE SISTEMAS E  
INFORMÁTICA**



**“Seguridad en Aplicaciones Informáticas”**

**INFORME DE TRABAJO PRÁCTICO DE SUFICIENCIA**

**PARA OPTAR EL TÍTULO DE:  
INGENIERO DE SISTEMAS E INFORMÁTICA**

**PRESENTADO POR EL BACHILLER:  
JUANITO AMASIFUEN SHUPINGAHUA**

**ASESOR:  
ING. RAFAEL VILCA BARBARAN**


**IQUITOS – PERÚ  
2015**

EXAMEN TÉCNICO DE SUFICIENCIA PREVIA ACTUALIZACIÓN ACADÉMICA APROBADO EN  
SUSTENTACIÓN PÚBLICA POR EL JURADO EXAMINADOR, DESIGNADO POR EL DECADO  
DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA DE LA UNIVERSIDAD  
NACIONAL DE LA AMAZONÍA PERUANA.

JURADOS:

  
.....  
Dr. Luis Benjamín Irigoin Sánchez  
Presidente

  
.....  
Ing. Alejandro Reategui Pezo.  
Primer Miembro

  
.....  
Ing. Tonny Eduardo Bardales Lozano  
Segundo Miembro



## PRESENTACIÓN

En la actualidad, la correcta administración y resguardo de la información es parte fundamental de cualquier empresa u organización, esto les permite la realización de sus actividades en forma rápida y eficiente, y por consiguiente una mejor rentabilidad.

Con los adelantos tecnológicos en el área computacional, área de comunicaciones y tecnologías de información, las empresas han optado por darle mayor importancia al uso de sistemas de información y estándares TIC, aprovechando los beneficios que estos les pueden otorgar en el procesamiento de la información en forma rápida y confiable, en la ayuda a toma de decisiones y adicionalmente en el proceso administrativo y productivo de la información.

Los problemas de seguridad en las aplicaciones, ya sea vulnerabilidades de los sistemas de información, seguridad perimetral, seguridad de la información y/o infraestructura de red, que puede desarrollar una empresa repercuten directamente en la imagen de la misma ante el mercado, afectando fuertemente su negocio. La correcta identificación y corrección de los posibles problemas de seguridad en una etapa temprana del desarrollo permite ahorrar trabajo, reducir los costos y aumentar la calidad de la aplicación final, mejorando el desempeño global.

El objetivo de este informe es deslindar en los principales conceptos y metodologías asociadas a la seguridad en el desarrollo de aplicaciones. Conocer los pilares fundamentales del enfoque en seguridad a la hora de desarrollar proyectos de aplicaciones y los estándares de calidad de administración TIC. Comprender y aplicar la gestión del riesgo en los proyectos de desarrollo, enfocados en la seguridad del producto, y la consistencia del proceso.



## RESUMEN

Este informe inicia con una serie de argumentos sobre la planificación de la seguridad en redes, indicando cada una de las variables a tener en cuenta al momento de la implementación de la misma, haciendo un énfasis en la planeación y las políticas a aplicar. Otro punto importante en esta parte, es que sintetiza los análisis de riesgo en la seguridad de una organización, los puntos importantes a tener en cuenta y que acciones tomar ante una vulnerabilidad.

La seguridad en aplicaciones no solo implica las estrategias de resguardo lógico de la información sino también del resguardo físico, por lo que se muestra una serie de conceptos de seguridad orientado a la seguridad de los activos informáticos y la política de uso para con los usuarios finales, así como su orientación y acuerdo de uso de los mismos.

La planeación estratégica y operativa de las Tecnologías de información y Comunicación es un factor muy puntual en el desarrollo del presente informe, abarcando desde la planificación del uso de los sistemas informáticos hasta establecer un plan de acción cuando se violen las políticas de seguridad. Mostrando un claro concepto de prevención.

Finalmente, como proceso de autocontrol, se establece parámetros muy definidos y claros sobre la importancia de llevar una auditoría sobre las TIC's en las organizaciones, mostrando una serie de pautas para desarrollar y planear la auditoría.



## ÍNDICE

|   |    |
|---|----|
| <b>PRESENTACIÓN</b> .....   | 2  |
| <b>RESUMEN</b> .....  | 3  |
| <b>ÍNDICE</b> .....   | 4  |
| <b>JUSTIFICACIÓN</b> .....  | 6  |
| <b>I. OBJETIVOS</b> .....   | 7  |
| <b>1.1. OBJETIVO GENERAL</b> .....  | 7  |
| <b>1.2. OBJETIVOS ESPECÍFICOS</b> .....   | 7  |
| <b>II. DESARROLLO DEL PROYECTO</b> .....  | 8  |
| <b>2.1. PLANEACIÓN DE SEGURIDAD EN REDES</b> .....  | 8  |
| <b>2.1.1. SEGURIDAD DE LA INFORMACIÓN</b> .....   | 9  |
| <b>2.2. VULNERABILIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS</b> .....                            | 11 |
| <b>2.2.1. AMENAZAS Y VULNERABILIDADES</b> .....   | 11 |
| <b>2.2.2. VULNERABILIDAD INFORMÁTICA</b> .....  | 14 |
| <b>2.2.3. CIBERSEGURIDAD</b> .....  | 16 |
| <b>2.3. PROTECCIÓN DE LOS SISTEMAS INFORMÁTICOS</b> .....                                     | 17 |
| <b>2.3.1. PRINCIPALES MÉTODOS DE PROTECCIÓN</b> .....   | 18 |
| <b>2.3.2. MEDIDAS APLICABLES EN CUALQUIER AMBIENTE</b> .....                                  | 19 |
| <b>2.4. POLÍTICAS DE SEGURIDAD</b> .....  | 21 |
| <b>2.4.1. OBJETIVOS DE UNA POLÍTICA DE SEGURIDAD</b> .....                                    | 22 |
| <b>2.4.2. MISIÓN, VISIÓN Y OBJETIVOS DE LA ORGANIZACIÓN</b> .....                             | 22 |
| <b>2.4.3. PLAN DE ACCIÓN CUANDO SE VIOLE LA POLÍTICA DE SEGURIDAD</b> .....                   | 24 |
| <b>2.4.4. PARÁMETROS PARA ESTABLECER POLITICAS DE SEGURIDAD DE LA INFORMACIÓN (PSI)</b> ..... | 25 |
| <b>2.4.5. RESPUESTA A LAS VIOLACIONES DE POLÍTICAS</b> .....                                  | 27 |
| <b>2.4.6. IDENTIFICACIÓN Y PREVENCIÓN DE PROBLEMAS DE SEGURIDAD</b> .....                     | 28 |
| <b>2.4.7. CONFIDENCIALIDAD</b> .....  | 29 |
| <b>2.5. IMPLEMENTACIÓN DE LAS POLÍTICA DE SEGURIDAD</b> .....                                 | 30 |
| <b>2.5.1. IMPLEMENTAR Y ESTRUCTURAR CONTROLES</b> .....                                       | 31 |
| <b>2.5.2. MODELO DE CONTROL DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN ÁREAS TIC</b> .....  | 33 |
| <b>2.5.3. PROCEDIMIENTOS Y PLANES DE CONTINGENCIA</b> .....                                   | 37 |
| <b>2.5.4. IMPLEMENTACIÓN PRÁCTICA DE UN PLAN DE CONTINGENCIA</b> .....                        | 40 |
| <b>2.5.5. POLÍTICAS DE SEGURIDAD FÍSICA</b> .....   | 42 |



|        |   |    |
|--------|---|----|
| 2.5.6. | NIVELES DE SEGURIDAD .....                            | 44 |
| 2.6.   | ETAPAS PARA IMPLEMENTAR UN SISTEMA DE SEGURIDAD ..... | 45 |
| 2.6.1. | ANÁLISIS DE RIESGO. ....                              | 46 |
| 2.6.2. | IDENTIFICACIÓN DE RECURSOS .....                      | 46 |
| 2.6.3. | IDENTIFICACIÓN DE LAS AMENAZAS .....                  | 47 |
| 2.6.4. | RIESGO DE REVELACIÓN DE INFORMACIÓN .....             | 48 |
| 2.7.   | AUDITORÍA DE SISTEMAS .....                           | 48 |
| 2.7.1. | PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA. ....       | 49 |
| 2.7.2. | CONTROL DE PROYECTOS.....                             | 50 |
| 2.7.3. | CONTROLES.....  | 50 |
| 2.8.   | SEGURIDAD EN CENTROS DE CÓMPUTO .....                 | 53 |
| 2.8.1. | ORDEN EN EL CENTRO DE CÓMPUTO. ....                   | 53 |
| 2.8.2. | SEGURIDAD LÓGICA Y CONFIDENCIAL .....                 | 53 |
| 2.8.3. | SEGURIDAD FÍSICA.....                                 | 54 |
| 2.8.4. | SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO. ....          | 55 |
| 2.8.5. | PROCEDIMIENTO DE RESPALDO EN CASO DE DESASTRE .....   | 57 |
| III.   | CONCLUSIONES.....                                     | 61 |
| IV.    | RECOMENDACIONES .....                                 | 62 |
| V.     | REFERENCIA BIBLIOGRÁFICA.....                         | 63 |



## JUSTIFICACIÓN

El acelerado incremento de la tecnología ha generado que las organizaciones se orienten hacia ellas, buscando afianzarse a un desarrollo sostenible y duradero.

Las tecnologías de información y comunicación (TIC's) han generado un alto índice del control de la productividad, dotando a las empresas de una rentabilidad controlada.

Estas TIC's generan ventaja competitiva a cada una de las empresas que se orientan a implementarlas como parte de la mejora en sus procesos; mejora, no solamente vista desde la perspectiva tecnológica, sino abarcando una mejora en todo aspecto competitivo.

El uso de herramientas tecnológicas se vuelve cada vez un punto de quiebre entre la supervivencia y la muerte de la organización, por lo que la investigación I + D, el control, el mantenimiento y la auditoria de estas herramientas se tornan fundamentales. En vista de ello, se generan múltiples variables y estándares para un buen manejo de las TIC's.

Por ello, en este informe, se pretende mostrar la estructura de control y operacional para la Seguridad de Sistemas y Aplicaciones en una organización. Esta estructura está orientado tanto a la seguridad física como también la seguridad lógica de los sistemas de información, así como también a la correcta orientación sobre el uso de los recursos al usuario final de los sistemas de información.



## I. OBJETIVOS

### 1.1. OBJETIVO GENERAL.

- ✓ Informar sobre la seguridad de aplicaciones informáticas y su importancia de su implementación en las organizaciones.

### 1.2. OBJETIVOS ESPECÍFICOS

- ✓ Describir las políticas, la planeación y el análisis de riesgo de la seguridad en redes.
- ✓ Identificar los recursos valiosos y las posibles vulnerabilidades de la infraestructura de red de la organización.
- ✓ Establecer parámetros para el diseño de la una política de red y de seguridad para la organización.
- ✓ Establecer las pautas para una correcta auditoria a la seguridad en aplicaciones para la organización.



## II. DESARROLLO DEL PROYECTO.

### 2.1. PLANEACIÓN DE SEGURIDAD EN REDES.

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la compañía. Vale la pena implementar una política de seguridad si los recursos y la información que la organización tiene en sus redes merecen protegerse. La mayoría de las organizaciones tienen en sus redes información delicada y secretos importantes; esto debe protegerse del acceso indebido del mismo modo que otros bienes valiosos como la propiedad corporativa y los edificios de oficinas.

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aún, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este mundo.

La información es un valor clave para cualquier institución ya sea pública o privada. La carencia de información o una información defectuosa pueden llevar la empresa a la ruina. Para que la empresa tenga éxito debe tener una información de calidad. Una información es de calidad cuando satisface los requerimientos que la gestión de la empresa le pide como son:

- ✓ La integridad.
- ✓ La fiabilidad.
- ✓ La confidencialidad.

La mayoría de los diseñadores de redes por lo general empiezan a implementar soluciones de firewall antes de que se haya identificado un problema particular de seguridad de red.

Quizá una de las razones de esto es que idear una política de seguridad de red efectiva significa plantear preguntas difíciles acerca de los tipos de servicios de inter redes y recursos cuyo acceso se permitirá a los usuarios, y cuales tendrán que restringirse debido a los riesgos de seguridad.



Si actualmente sus usuarios tienen acceso irrestricto a la red, puede ser difícil aplicar una política que limite ese acceso. También debe tomar en cuenta que la política de seguridad que Usted debe usar es tal, que no disminuir la capacidad de su organización. Una política de red que impide que los usuarios cumplan efectivamente con sus tareas, puede traer consecuencias indeseables: los usuarios de la red quizá encuentren la forma de eludir la política de seguridad, lo cual la vuelve inefectiva.

Una política de seguridad en redes efectiva es algo que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar.

### **2.1.1. SEGURIDAD DE LA INFORMACIÓN.**

El objetivo de la seguridad es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas o de la información contenida en ellos, así como tratando de proteger las redes privadas y sus recursos mientras que se mantienen los beneficios de la conexión a una red pública o a una red privada.

La seguridad tiene su nacimiento con la aparición de los ataques a la información por parte de intrusos interesados en el contenido de ésta.

El objetivo de la seguridad de la información es:

- ✓ Mantener el secreto, evitando los accesos no autorizados.
- ✓ Mantener la autenticidad, evitando modificaciones no autorizadas.

Dentro del concepto de seguridad debemos distinguir la Seguridad Física de la Seguridad Lógica, y para tener un concepto más claro, detallaremos a continuación cada una de ellas.

#### **a. Seguridad Física.**

La seguridad física comprende el aspecto del hardware, la manipulación del mismo, así como también el ambiente en el cual se van a instalar los equipos.



Para garantizar la seguridad de los mismos podríamos considerar los siguientes criterios:

- Uso de equipo personal autorizado.
- Solo podrá tener acceso al equipo aquella persona que cuente con conocimientos mínimos sobre computación.
- Tener más de un servidor de **base de datos**, lo cual asegurará la integridad total de la información.
- Ubicación de las instalaciones, la cual debe cumplir las normas internacionales de calidad (ISO 27001).
- Control de alarma la cual notifique en todo momento sobre la integridad física del sistema.

**b. Seguridad Lógica.**

La seguridad lógica comprende el aspecto de los sistemas, tanto operativo como de información. Dentro de las medidas a tomar para garantizar la seguridad de los mismos se recomienda las siguientes:

- Construcción de contraseñas en diversos niveles del sistema, donde permita solo el acceso en base a niveles de seguridad de usuarios con permiso.
- En base al sistema operativo que use como plataforma, utilizar algoritmos que generen claves para poder encriptar los archivos de contraseñas dentro del sistema, me permita mayor seguridad en un entorno de red.
- Generar un módulo del sistema para la emisión de reportes para el administrador del sistema, en donde se muestre tablas de uso del sistema, usuarios y los niveles de acceso por parte de los tales para poder determinar el uso y acceso al sistema.
- Es necesario contar con el diseño de módulos que ejecuten un control de alarma la cual notifique en todo momento sobre la integridad de la información del sistema.



## 2.2. VULNERABILIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS

La vulnerabilidad informática es una de las principales desventajas a la que las empresas se encuentran expuestas poseen. Un incidente de vulnerabilidad informática puede no solo denegar el servicio a los consumidores, sino provocar la pérdida de los datos confidenciales de la empresa, ante un robo de información o una maniobra maliciosa de competencia desleal en el ámbito comercial.

### 2.2.1. AMENAZAS Y VULNERABILIDADES.

#### a. Amenazas.

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Para mostrar algunas de las amenazas más preocupantes, consultamos dos estadísticas, el primer grafo es resultado de la “Encuesta sobre Seguridad y Crimen de Computación – 2012” del Instituto de Seguridad de Computación (CSI por sus siglas en inglés) que base en 433 respuestas de diferentes entidades privadas y estatales en los EE.UU.

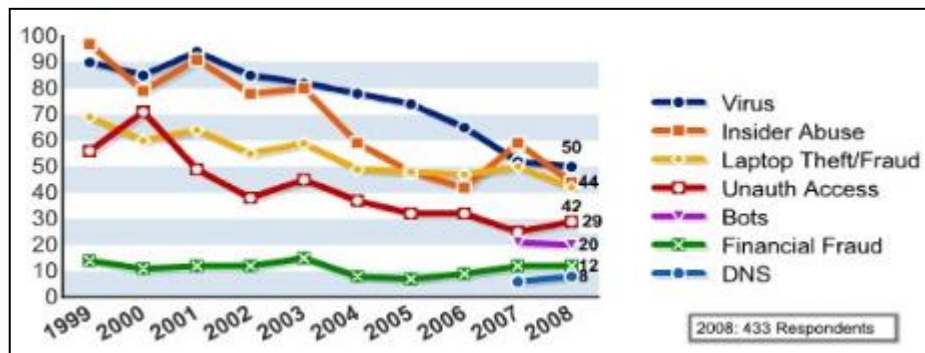


Gráfico N° 01: Encuesta sobre Seguridad y Crimen de Computación – 2012

El segundo tiene su origen en una encuesta que se hizo en el año 2013, con 34 organizaciones sociales a nivel sudamericano.

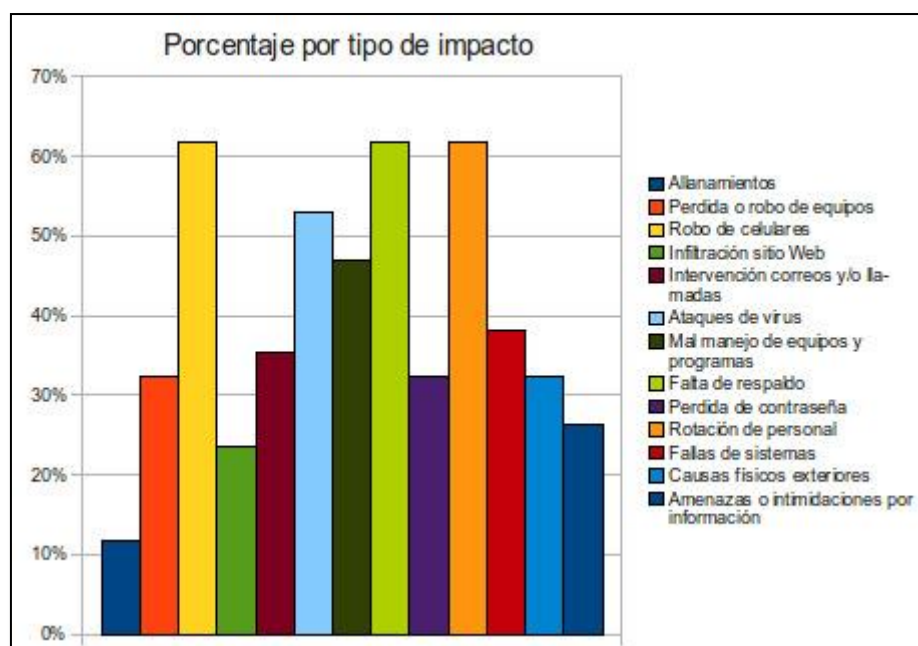




Gráfico N° 02: Nivel Sudamericano.

Como se observa, existen algunas similitudes respecto a las amenazas más preocupantes:

- ✓ Ataques de virus (>50%).
- ✓ Robo de celulares, portátiles y otros equipos (>40%).

Pero también existen otras amenazas que, aunque no aparezcan en ambas encuestas, son muy alarmantes y que se debe tomar en consideración.

- ✓ Falta de respaldo de datos.
- ✓ Perdida de información por rotación, salida de personal.
- ✓ Abuso de conocimientos internos (no consultado en encuesta de organizaciones sociales).
- ✓ Mal manejo de equipos y programas.
- ✓ Accesos no autorizados.

**b. Vulnerabilidades.**

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras



palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Política.

### **2.2.2. VULNERABILIDAD INFORMÁTICA.**

La vulnerabilidad de los sistemas informáticos las podemos agrupar en función de:

#### **Diseño.**

1. Debilidad en el diseño de protocolos utilizados en las redes.
2. Políticas de seguridad deficientes.

#### **Implementación.**

3. Errores de programación.
4. Existencia de puertas traseras en los sistemas informáticos.
5. Descuido de los desarrolladores.

#### **Uso.**

6. Configuración inadecuada de los sistemas informáticos.
7. Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
8. Disponibilidad de herramientas que facilitan los ataques.

#### **Vulnerabilidad del día cero.**

9. Cuando no exista una solución conocida para la vulnerabilidad, pero si se conoce como explotarla.

Globalmente clasificamos las vulnerabilidades en:



**a. Vulnerabilidades de desbordamiento de buffer.**

Se produce cuando un programa no controla la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Se puede aprovechar para ejecutar código que nos de privilegios de administrador.

**b. Vulnerabilidades de condición de carrera (race condition).**

La condición de carrera se da principalmente cuando varios procesos acceden al mismo tiempo a un recurso compartido, por ejemplo una variable, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma.

**c. Vulnerabilidades de error de formato de cadena (format string bugs).**

La principal causa de los errores de cadena de formato es aceptar sin validar la entrada de datos proporcionada por el usuario.

Es un error de programación y el lenguaje más afectado es C/C++. Un ataque puede conducir de manera inmediata a la ejecución de código arbitrario y a la revelación de información.

**d. Vulnerabilidades de Cross Site Scripting (XSS).**

Abarcaban cualquier ataque que permitiera ejecutar scripts como VBScript o JavaScript, en el contexto de otro sitio web. Estos errores se pueden encontrar en cualquier aplicación que tenga como objetivo final presentar la información en un navegador web.

Un uso de esta vulnerabilidad es hacer phishing. La víctima ve en la barra de direcciones un sitio, pero realmente está en otro. La víctima introduce su contraseña y se la envía al atacante.

**e. Vulnerabilidades de Inyección SQL.**



Una inyección SQL se produce cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.

**f. Vulnerabilidades de denegación del servicio.**

La denegación de servicio provoca que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

**g. Vulnerabilidades de ventanas engañosas (Window Spoofing).**

Las ventanas engañosas son aquellas que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que des información. Hay otro tipo de ventanas que, si las sigues, obtienen datos del ordenador para luego realizar un ataque.

**2.2.3. CIBERSEGURIDAD**

El traslado de la actividad de todos los actores de la sociedad al ciberespacio, ha aumentado drásticamente su exposición a nuevos riesgos y amenazas. Por ello el concepto ciberseguridad, cuyo objetivo es la protección de las organizaciones y las instituciones contra los ataques que los cibercriminales lanzan para comprometer sus sistemas de información a nivel de hardware o software y contra el robo o destrucción de la información que almacenan o gestionan.

La ciberseguridad ya es una prioridad en la agenda de los gobiernos y de las empresas de todo el mundo.

En 2014, nueve grandes organizaciones sobre diez han tenido algún tipo de brecha de seguridad con un coste medio anual para las organizaciones que se sitúa cerca de los 15 millones de dólares.

Un 46% de las organizaciones espera sufrir un ataque a lo largo del 2015 y 2016.



La profesionalización de los atacantes y la sofisticación y violencia de los ataques hacen que la simple protección ya no sea suficiente, sino que sea necesario poner en marcha medidas de monitorización constante orientadas a la detección y prevención de los ataques, mucho antes de que estos tengan lugar, así como de mecanismos de respuestas adecuados.

Estos mecanismos deben tener un enfoque multidisciplinario, en cuanto que la ciberseguridad trasciende de la dimensión puramente tecnológica y depende de muchos más factores internos y externos, siendo el factor humano uno de los más importantes: el 75% de las grandes organizaciones han sufrido incidentes de seguridad relacionados con acciones o comportamientos de sus empleados.

El mercado global de la ciberseguridad está en continuo crecimiento y se espera que alcance los 170 mil millones de dólares en 2025, a una tasa de crecimiento compuesta anual del 9,8%. La seguridad gestionada, los servicios basados en la nube, la protección de datos en movilidad, el BYOD, las amenazas persistentes avanzadas (APT), Internet de las cosas y la seguridad en smart grid son algunos de los segmentos que experimentarán más crecimiento.

Para hacer frente a las ciberamenazas, el 37% de las organizaciones planea emplear más profesionales de ciberseguridad a lo largo de 2015, aunque el 92% de ellas espera encontrar dificultades en encontrar candidatos con las competencias adecuadas. A nivel global se ha estimado un déficit de más de un millón de profesionales de ciberseguridad.

### **2.3. PROTECCIÓN DE LOS SISTEMAS INFORMÁTICOS**

Lo primero que hemos de hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.



A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir.

La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

### **2.3.1. PRINCIPALES MÉTODOS DE PROTECCIÓN**

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda (proactividad).

Métodos de Protección:

#### **a. Sistema de detección de intrusos.**

Son sistemas que permiten analizar las bitácoras de sistemas en busca de patrones de comportamientos o eventos que puedan considerarse sospechosos, en base a la información con la que han sido previamente alimentados.

#### **b. Sistemas orientados a conexión de red.**

Se consideran a los cortafuegos (Firewall) y los wrappers, los cuales monitorean las conexiones de red que se intentan establecer con una red o equipo en particular, siendo capaces de efectuar una acción en base a datos como: origen de la conexión, destino de la



conexión, servicio solicitado, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta la alerta al administrador vía correo electrónico.

**c. Sistemas de análisis de vulnerabilidades.**

Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. Las desventajas de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que busquen acceso no autorizado al sistema.

**d. Sistemas de protección a la privacidad de la información.**

Herramientas que utilizan criptografía para asegurar que la información solo es visible a quien tiene autorización a verla. Su aplicación es principalmente en comunicaciones entre dos entidades. Dentro de este tipo de herramientas podemos situar a Petty Good Privacy (PGP), Secure Sockets Layer (SSL) y los Certificados digitales.

**e. Sistemas de protección a la integridad de información.**

Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alter5aciones indeseadas en la información que se intenta proteger.

Algunos ejemplos son los programas que implementan algoritmos como MESSage Digest 5 (MD5) o Secure Hass Algorithm 1 (SHA-1), o bien sistemas que utilizan varios de ellos como Tripwire.

**2.3.2. MEDIDAS APLICABLES EN CUALQUIER AMBIENTE.**

**a. Informar al usuario/administrador.**

El administrador, debe notificar a sus usuarios de los mecanismos de seguridad que se han implementado, y animar a los usuarios a utilizar estos mecanismo de seguridad, dando a conocer las posibles consecuencias de no cumplir con ellos. El usuario por otra parte, debe considerar todas las disposiciones y recomendaciones que



brinda el Administrador de los sistemas, además el usuario debe hacer conocer al administrador cualquier sospecha de violación de cualquier recurso al que el usuario tiene acceso legítimo.

**b. Recuperación: Copias de Seguridad.**

Los mecanismos preventivos pueden evitar muchos problemas y ataques pero no garantizan estar exentos de todo riesgo o daño. Tras detectar que la seguridad ha sido comprometida, una de las tareas del administrador de sistemas afectado será recuperarlo y dejarlo tal y como estaba antes de incidente.

Lo primero que un administrador debe realizar a la hora de diseñar un sistema de copias de seguridad es planificar la estrategia a seguir para cumplir la política de seguridad de la organización.

Ejemplo: en un ambiente universitario dedicado a aulas de prácticas de informática, se pueden establecer que las copias de seguridad afecten, exclusivamente a los sistemas de ficheros de los equipos de las aulas.

De esta forma, ante una posible caída (situación bastante probable) se pueden recuperar los equipos en el menor tiempo posible pero se pierden los datos de los usuarios.

**c. Realizar Verificaciones no predecibles.**

Si se hacen verificaciones periódicas, y alguien más conoce cómo y cuándo se realizan estas verificaciones, entonces será necesario además hacer verificaciones de periodicidad no predecible, a fin de obtener una estadística más real del comportamiento del sistema.

**d. Leer Bitácoras.**

Las bitácoras del sistema reflejan lo que ocurre en el mismo. De nada sirve tenerlas si no son leídas. Ahí es donde pueden descubrirse ataques no exitosos perpetrados contra su sistema.



**e. Aplicar “Parches” o tener las últimas versiones de software.**

Las vulnerabilidades sobre algún producto o plataforma, pueden dar la vuelta al mundo rápidamente gracias a Internet. Es recomendable por ello contar siempre con la versión más actualizada del software, o bien aplicar los “parches” respectivos cuando son liberados. En este rubro, el software libre (Linux/Apache) cuenta con una ventaja sobre software comercial, pues el tiempo de respuesta es dramáticamente más rápido para el software libre.

**f. Cancelación de Cuentas de Accesos.**

Todo lo anterior no sirve si las personas que han trabajado para la institución poseen sus cuentas de acceso después de haber dejado de colaborar con ella. Las estadísticas demuestran que un 85% de los ataques de seguridad son realizados desde dentro de la institución, o bien a través de cuentas personales que estuvieron dentro de ella.

## **2.4. POLÍTICAS DE SEGURIDAD**

Las políticas son una serie de instrucciones documentadas que indican la forma en que se llevan a cabo determinados procesos dentro de una organización, también describen cómo se debe tratar un determinado problema o situación. Las políticas pueden considerarse como un conjunto de leyes obligatorias propias de una organización, y son dirigidas a un público mayor que las normas pues las políticas proporcionan las instrucciones generales, mientras que las normas indican requisitos técnicos específicos. Las normas, por ejemplo, definirían la cantidad de bits de la llave secreta que se requieren en un algoritmo de cifrado. Por otro lado, las políticas simplemente definirían la necesidad de utilizar un proceso de cifrado autorizado cuando se envíe información confidencial a través de redes públicas, tales como Internet.

Esquemáticamente.

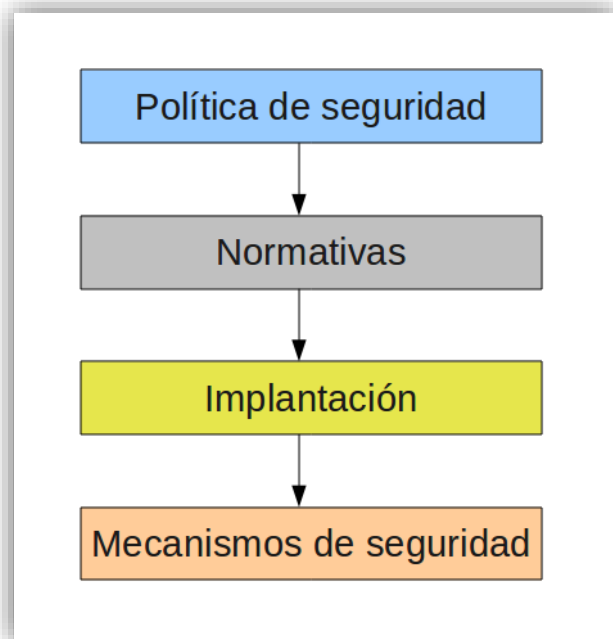


Gráfico N°03. Fuente: aulamentor – Gobierno de España

### **Mecanismos de Seguridad.**

Se dividen en tres grupos:

1. Prevención: evitan desviaciones respecto a la política de seguridad.
2. Detección: detectan las desviaciones si se producen.
3. Recuperación: se aplican cuando se han detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento

#### **2.4.1. OBJETIVOS DE UNA POLÍTICA DE SEGURIDAD**

El objetivo de una política de seguridad informática es la de implantar una serie de leyes, normas, estándares y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos aquellos miembros de la organización a las que van dirigidos.

#### **2.4.2. MISIÓN, VISIÓN Y OBJETIVOS DE LA ORGANIZACIÓN MISIÓN.**



Una misma organización puede tener varias misiones, que son las actividades objetivas y concretas que realiza. Las misiones también pretenden cubrir las necesidades de la organización.

La misión es influenciada en momentos concretos por algunos elementos como: la historia de la organización, las preferencias de la gerencia y/o de los propietarios, los factores externos o del entorno, los recursos disponibles, y sus capacidades distintivas.

### **VISIÓN.**

Es la imagen idealizada de lo que se quiere crear. Tal idea debe estar bien definida, pues todas las actividades de la organización estarán enfocadas a alcanzar esta visión.



### **OBJETIVOS.**

Son actividades específicas enfocadas a cumplir metas reales, alcanzables y accesibles. Se puede decir que un objetivo es el resultado que se espera logra al final de cada operación.

Así, se vuelve importante considerar la misión, la visión y el objetivo de ser de la empresa, a fin de realizar un estudio que con base en éstas permita identificar el conjunto de políticas de seguridad informática que garantice la seguridad, confidencialidad y disponibilidad de la información.

#### **2.4.3. PLAN DE ACCIÓN CUANDO SE VIOLE LA POLÍTICA DE SEGURIDAD**

Cada vez que se viola la política de seguridad, el sistema está sujeto a amenazas. Si no se producen cambios en la seguridad de la red cuando esta sea violada, entonces debe modificarse la política de seguridad para eliminar aquellos elementos que no sean seguros.

La política de seguridad y su implementación deben ser lo menos obstructivas posible. Si la política de seguridad es demasiado restrictiva, o esta explicada inadecuadamente, es muy probable que sea violada o desactivada.

Al margen del tipo de política que se implemente, algunos usuarios tienen la tendencia a violarla. En ocasiones las violaciones a la política son evidentes; otras veces estas infracciones no son detectadas. Los procedimientos de seguridad que usted establezca deben reducir al mínimo la posibilidad de que no se detecte una infracción de seguridad.

Cuando usted detecte una violación a la política de seguridad, debe determinar si esta ocurrió debido a la negligencia de un individuo, a un accidente o error, por ignorancia de la política vigente o si deliberadamente la política fue pasada por alto. En este último caso, la



violación quizás haya sido efectuada no solo por una persona, sino por un grupo que a sabiendas realiza un acto en violación directa de la política de seguridad. En cada una de estas circunstancias, la política de seguridad debe contar con lineamientos acerca de las medidas que se deben tomar.

Debe llevarse a cabo una investigación para determinar las circunstancias en torno a la violación de seguridad, y cómo y por qué ocurrió. La política de seguridad debe contener lineamientos acerca de las acciones correctivas para las fallas de seguridad. Es razonable esperar que el tipo y severidad de la acción dependan de la gravedad de la violación.

#### **2.4.4. PARÁMETROS PARA ESTABLECER POLITICAS DE SEGURIDAD DE LA INFORMACIÓN (PSI)**

La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, por ende, debe estar avalado y contar con un fuerte apoyo de la dirección y/o máxima gerencia, ya que sin este apoyo, su implementación será más compleja e incluso puede fracasar.

Es importante que al momento de formular las políticas de seguridad de la información, se consideren por lo menos los siguientes aspectos:

- a. Efectuar un análisis de riesgos informáticos para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- b. Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- c. Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.



- d. Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en proteger los activos críticos en su área.
- e. Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios de políticas puedan actualizarse oportunamente.
- f. Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

#### **Razones que impiden la aplicación de las políticas de seguridad informática.**

Se debe ser capaz de convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática, sino los esfuerzos de su implementación pueden ser desperdiciados.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos de las empresas a no comprender exactamente la razón o motivos de las inversiones.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensible y por ende su imagen.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencia en las proyecciones y utilidades de la compañía.



Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

#### **2.4.5. RESPUESTA A LAS VIOLACIONES DE POLÍTICAS**

Cuando ocurre una violación, la respuesta puede depender del tipo de usuario responsable del acto. Las violaciones a la política pueden ser cometidas por gran variedad de usuarios; algunos pueden ser locales y otros externos. Los usuarios locales son llamados usuarios internos y los externos, usuarios foráneos. Por lo general, la distinción entre ambos tipos está basada en los límites de red, administrativos, legales o políticos. El tipo de límite determina cual debe ser la respuesta a la violación de la seguridad. Los ejemplos de respuestas pueden ir desde una reprimenda o advertencia verbal, una carta formal o la presentación de cargos judiciales.

Usted necesita definir la acción según el tipo de violación. Estas acciones requieren ser definidas con claridad, con base en el tipo de usuario que haya violado la política de seguridad de cómputo. Los usuarios internos y externos de su red deben estar conscientes de la política de seguridad. Si hay usuarios externos que utilicen legalmente la red, es responsabilidad de usted verificar que esas personas conozcan las políticas que se han establecido. Esto es de particular importancia si usted tiene que emprender acciones legales en contra de los transgresores.

Si se ha producido una pérdida significativa, quizá usted tendrá que tomar acciones más drásticas. Si todo esto implica una publicidad



negativa, quizás usted prefiera arreglar la falla de seguridad y no emprender acción judicial.

El documento de la política de seguridad también debe contener procedimientos para manejar cada tipo de incidente de violación. Debe llevarse un registro apropiado de tales violaciones, el cual ha de revisarse periódicamente para observar tendencias y tal vez ajustar la política de seguridad para que dicha política tome en cuenta cualquier nuevo tipo de amenaza.

#### **2.4.6. IDENTIFICACIÓN Y PREVENCIÓN DE PROBLEMAS DE SEGURIDAD**

La política de seguridad define lo que necesita protegerse, pero no señala explícitamente como deben protegerse los recursos y el enfoque general para manejar los problemas de seguridad. En una sección separada de la política de seguridad deben abordarse los procedimientos generales que deben implementarse para evitar problemas de seguridad.

La política de seguridad debe remitirse a la guía del administrador de sistemas del sitio respecto a detalles adicionales acerca de la implementación de los procedimientos de seguridad.

Antes de establecer los procedimientos de seguridad, debe evaluar el nivel de importancia de los recursos de la red y su grado de riesgo.

En muchas ocasiones es tentador empezar a implementar procedimientos como el siguiente, sin haber definido la política de seguridad de la red: **“Nuestro sitio necesita ofrecer a los usuarios acceso telnet a los hosts internos y externos, evitar acceso NFS a los hosts internos, pero negarlo a los usuarios externos, tener tarjetas inteligentes para registrarse desde afuera, tener módems de contestación de Llamada...”** Si no se conocen adecuadamente los recursos más importantes y los que están expuestos a mayores riesgos, el enfoque anterior hará que ciertas áreas tengan más protección de la



que necesitan, y que otras áreas más importantes no tengan suficiente protección.

Establecer una política de seguridad eficaz requiere considerable esfuerzo. Se necesita cierto esfuerzo para considerar todos los aspectos y cierta disposición para establecer las políticas en papel y hacer lo necesario para que los usuarios de la red la entiendan adecuadamente.

#### **2.4.7. CONFIDENCIALIDAD**

La confidencialidad puede definirse como el hecho de mantener las cosas ocultas o secretas. Esta es una consideración muy importante para varios tipos de datos delicados.

Las siguientes son algunas de las situaciones en las que la información es vulnerable de ser divulgada:

- ✓ Cuando la información está almacenada en un sistema de cómputo.
- ✓ Cuando la información está en tránsito hacia otro sistema en la red.
- ✓ Cuando la información está almacenada en cintas de respaldo o discos magnéticos.

El acceso a la información que está almacenada en una computadora está controlado mediante los permisos de archivo, las listas de control de acceso (ACL) y otros mecanismos similares.

La información en tránsito puede protegerse mediante la encriptación o los gateways de las firewalls. La encriptación puede usarse para proteger la información en las tres situaciones.

El acceso a la información almacenada en cintas o discos magnéticos puede controlarse mediante la seguridad física; como puede ser, guardar las cintas en una caja de seguridad o en una red inaccesible.



## 2.5. IMPLEMENTACIÓN DE LAS POLÍTICA DE SEGURIDAD

La implementación de medidas de seguridad, es un proceso Técnico-Administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Se deberá tener en cuenta que la implementación de Políticas de Seguridad, trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. La implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativamente.

Por esto, será necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Una PSI deberá abarcar:

- ✓ Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- ✓ Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- ✓ Responsabilidad de cada uno de los servicios, recurso y responsables en todos los niveles de la organización.
- ✓ Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- ✓ Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
- ✓ Definición de violaciones y las consecuencias del no cumplimiento de la política.



- ✓ Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud qué pasara o cuándo algo sucederá; ya que no es una sentencia obligatoria de la ley.
- ✓ Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porqué de las decisiones tomadas.
- ✓ Finalmente, como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

Una proposición de una forma de realizar una PSI adecuada puede apreciarse en el siguiente diagrama:

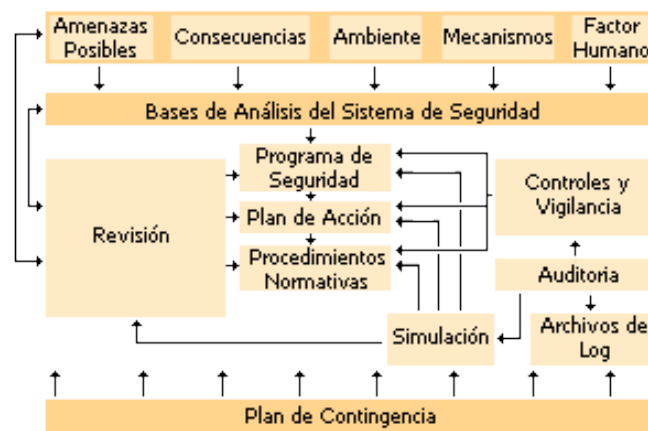


Gráfico N° 04.

Fuente:

Manual de Seguridad en Redes. <http://www.arcert.gov.ar>

### 2.5.1. IMPLEMENTAR Y ESTRUCTURAR CONTROLES.

Con el propósito de enfrentar correctamente los procesos de auditoría y a la vez para satisfacer un adecuado nivel de control interno en las actividades de TIC, se deben diseñar controles, de manera que ellos abarquen a todos los procesos que se manejan por medio de las TIC en una organización. En todo proceso el OSI juega un papel de relevancia,



puesto que con su experiencia se pueden realizar estas implementaciones de forma adecuada y con la relevancia que la organización requiere.

En sí, los controles deben estar contruidos en base a áreas (procesos) y objetivos de control de los cuales se deben desprender las actividades y finalmente los controles en sí. Por ejemplo la norma ISO/ IEC 27002 describe 39 objetivos de control. Sin embargo, otras normas o estándares como ISO 17799, ITIL y COBIT proponen un número distinto de controles.

De manera de apoyar la implementación del modelo propuesto y de modo de hacer práctico el proceso de estructurar e implementar controles, el modelo entrega una estructura, con una base de 85 objetivos de control los cuales nacen 120 controles generales para TIC. Esta base de controles debe ser ajustada según el ámbito de la organización y los alcances de sus actividades en TIC.

Estos controles han sido establecidos conforme el estudio de los estándares antes citados, considerando especialmente las indicaciones de ISO 17799 e ISO/IEC 27002, y pretenden ser una guía para quien estime su activación. **Es importante recalcar que los controles en si no bastan para tener un correcto gobierno TI**, ya que ello solo se puede alcanzar cuando existe todo el marco compuesto por políticas, procedimientos, informes, registros, instructivos y controles.

Las organizaciones que tienen mayor interés en asegurar y demostrar menor riesgo son las instituciones y organizaciones bancarias y/o financieras, debido a que el activo de información en este caso puede efectivamente determinar la continuidad de sus operaciones. Ellas están en obligación de implementar estándares y metodología de clase mundial que permitan el resguardo a sus clientes.



## 2.5.2. MODELO DE CONTROL DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN ÁREAS TIC.

Si bien el modelo PDCA es el estándar formal de ISO, éste se construye sobre una base que no necesariamente se aplica a todas las organizaciones, sobre todo cuando estas no se han involucrado en procesos relacionados con normas ISO, por ello, con una base práctica se presenta el siguiente modelo, el cual no omite ni restringe las actividades señaladas en el modelo formal, sino que se vale de ellas para sustentar un formato práctico de actividades que deben ser abarcadas para lograr un adecuado nivel de seguridad de la información en las áreas de TIC en cualquier tipo de organización.

Este modelo puede ser perfeccionado y modificado en el futuro dado que su estructura se debe ajustar a los contrastantes cambios que surgen de las organizaciones como sistema dinámico.

Las particularidades del modelo que se presenta a continuación residen en su aspecto operativo y práctico, puesto que se considera su estructuración, formación e implementación bajo dos grandes fases:

- ✓ Fase de Elaboración.
- ✓ Fase de Aplicación.

Estas fases contemplan el conjunto de actividades que de ellas se desprenden y están ligadas mediante la secuencia de actividades que es necesario desarrollar a fin de elaborar y aplicar correctamente el modelo.

Este modelo considera los principales elementos incluidos en las diversas normas y estándares internacionales relacionados con la seguridad de la información, por lo que creemos que apoya la concreción de un “Gobierno de TIC”, lo que a su vez abarca un aspecto



mayor al que su diseño se orientó inicialmente, ya que esto implica que no solo cubre temas de seguridad y de riesgos, sino a que al mismo tiempo apoya a lograr aspectos de estructura organizaciones, descripciones de cargo y tareas, definiciones de misión y visión, o solo a nivel gerencial, sino que a nivel de cada área de TI.

La siguiente presenta el modelo en forma esquemática. El esquema presentado resume y agrupa todas las actividades y se debe entender que muchas de ellas llevarán un ciclo continuo de mejora.

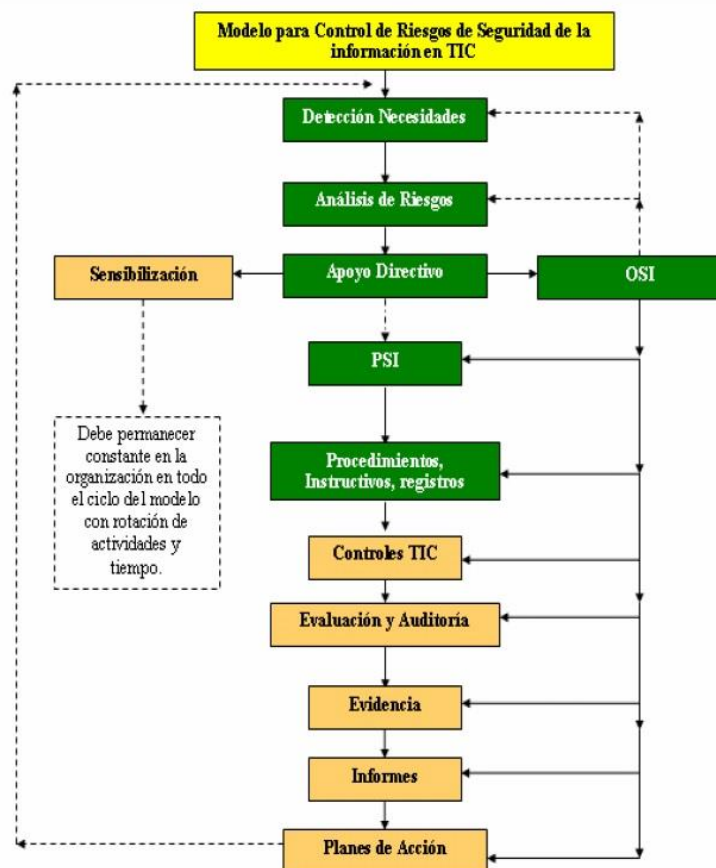




Gráfico N° 05. Modelo de Control de Riesgos de Seguridad de la Información en Áreas de TIC.

Las actividades son secuenciales y a la vez se comportan en un estado cíclico con periodos de tiempos en su ciclo que varían dependiendo de cada organización y del estado de avance que ella tenga respecto a temas de seguridad de la información.

La descripción de cada una de las fases y actividades que se consideran en el gráfico sería:

1. Detección de Necesidades: corresponde al levantamiento de todas las actividades relacionadas con los impactos que la organización pueda tener en relación con su seguridad de la información.
2. Análisis de Riesgo: corresponde a evaluar todos los potenciales riesgos en los cuales se pueda ver envuelta la organización por aspectos emanados de las TIC y que impactan en la seguridad de la información.
3. Apoyo Directivo: corresponde a la presentación del resultado de las etapas anteriores con el fin de conseguir el apoyo para concretar la implementación de la seguridad de la información (presupuestos, personal, capacitación, etc.).
4. OSI: la organización debe designar a un OSI para que realice, apoye, dirija y pueda llevar el control de implementación y posterior seguimiento a todo el modelo de seguridad de la información. Además el OSI estará presente en todas las actividades y con énfasis en la fase de aplicación en la cual participara en forma activa en todas las actividades que se indican en adelante.
5. Confección PSI: corresponde al diseño de las Políticas de Seguridad de la Información.
6. Confección de procedimientos, instructivos y registros: corresponde al desarrollo de documentos que formalicen como se



- deben realizar las actividades y que información es que se debe retener como evidencia para dar conformidad a las PSI.
7. Controles TIC: en esta etapa se diseñan y definen los procesos, objetivos de control, controles y evidencias formales de las actividades de seguridad que darán sustento a los procesos de revisión o auditorias del modelo.
  8. Evaluación y auditoria: en esta etapa se debe realizar, preparar y desarrollar la revisión que avale que todos los procesos de TI se están cumpliendo y llevando a cabo adecuadamente, lo cual será evaluado por el mismo proceso de auditoria (interna y/o externa).
  9. Evidencia: en esta etapa se busca verificar de manera adecuada que todos los registros de TI para todos sus procesos y controles estén disponibles para cualquier tipo de revisión, particularmente a los procesos de auditoría.
  10. Informes: en esta etapa se contempla la confección de informes del proceso de revisión que derivan en actividades de mejora al modelo y con revisiones por parte de la dirección de la organización que permitan confeccionar adecuados planes de acción.
  11. Planes de Acción: esta etapa consiste en la aplicación de los planes de acción conforme a los plazos y actividades que fueron indicados en el proceso de auditoría. Estos planes pueden confirmar la revisión y ajuste de todo tipo de actividades ya sea a nivel de procesos de seguridad, de evidencias, de políticas o de cualquier otra actividad que sea identificada.
  12. Sensibilización: esta etapa permite entregar constante información a la organización sobre la importancia de mantener la seguridad de la información y el resguardo de todas las actividades de TI.



### 2.5.3. PROCEDIMIENTOS Y PLANES DE CONTINGENCIA.

#### PLAN DE CONTINGENCIA.

Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

El plan de contingencia propone una serie de procedimientos alternativos al funcionamiento normal de la organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia externa.

Solo cuando una organización toma conciencia de lo importante que es la seguridad de sus recursos incluyendo sus tecnologías de la información, es cuando empieza a diseñar y establecer medidas de seguridad que tienen por objetivo protegerla de diversas situaciones perjudiciales.

Aunque prevenir éstos desastres es de vital importancia, tampoco se puede descuidar la casi inevitable eventualidad de que sucedan, para ello también se necesita formular y establecer una serie de procedimientos que permitan enfrentar los problemas y posteriormente restaurar las condiciones normales de operación del área afectada.

#### Etapas del Plan.

- Análisis de Riesgo.
- Plan de Respaldo.
- Plan de Recuperación.
- Plan de Mantenimiento.
- Plan de Entrenamiento.

#### Plan de Contingencia aplicada a la seguridad en aplicaciones Informáticas.

Un punto importante que no tiene que ser obviado en el desarrollo de un Plan de Contingencia, es disponer de puntos que contemplen la



protección y el aseguramiento del funcionamiento óptimo de las aplicaciones informáticas de la organización. La estabilidad funcional de las aplicaciones se considera un factor crucial en una institución tecnificada, o dicese de otro modo, las aplicaciones informáticas se han vuelto tan importante que su dependencia está ligada con la muerte o levantamiento de la organización.

Se deben de considerar los siguientes puntos en el desarrollo de un Plan de Contingencia:

- Análisis de Riesgo de software.
- Prioridades de protección.
- Accesos no autorizados.
- Desastres naturales.
- Vandalismo.
- Fallas de Personal clave.
- Fallas de Hardware y Software.
  - ✓ Fallas en el servidor de aplicaciones y de base de datos.
  - ✓ Fallas en la infraestructura de red.
  - ✓ Fallas en el Firewall.
- Plan de Acción.
  - ✓ Realizar un levantamiento de los servicios informáticos.
  - ✓ Identificar un conjunto de amenazas.
  - ✓ Revisar la seguridad, controles físicos y ambientales existentes.
  - ✓ Identificar los servicios fundamentales del área de sistemas informáticos de la empresa

**Ejemplo Diagrama de Respuesta de emergencia de “FALLAS EN HARDWARE Y SOFTWARE”**

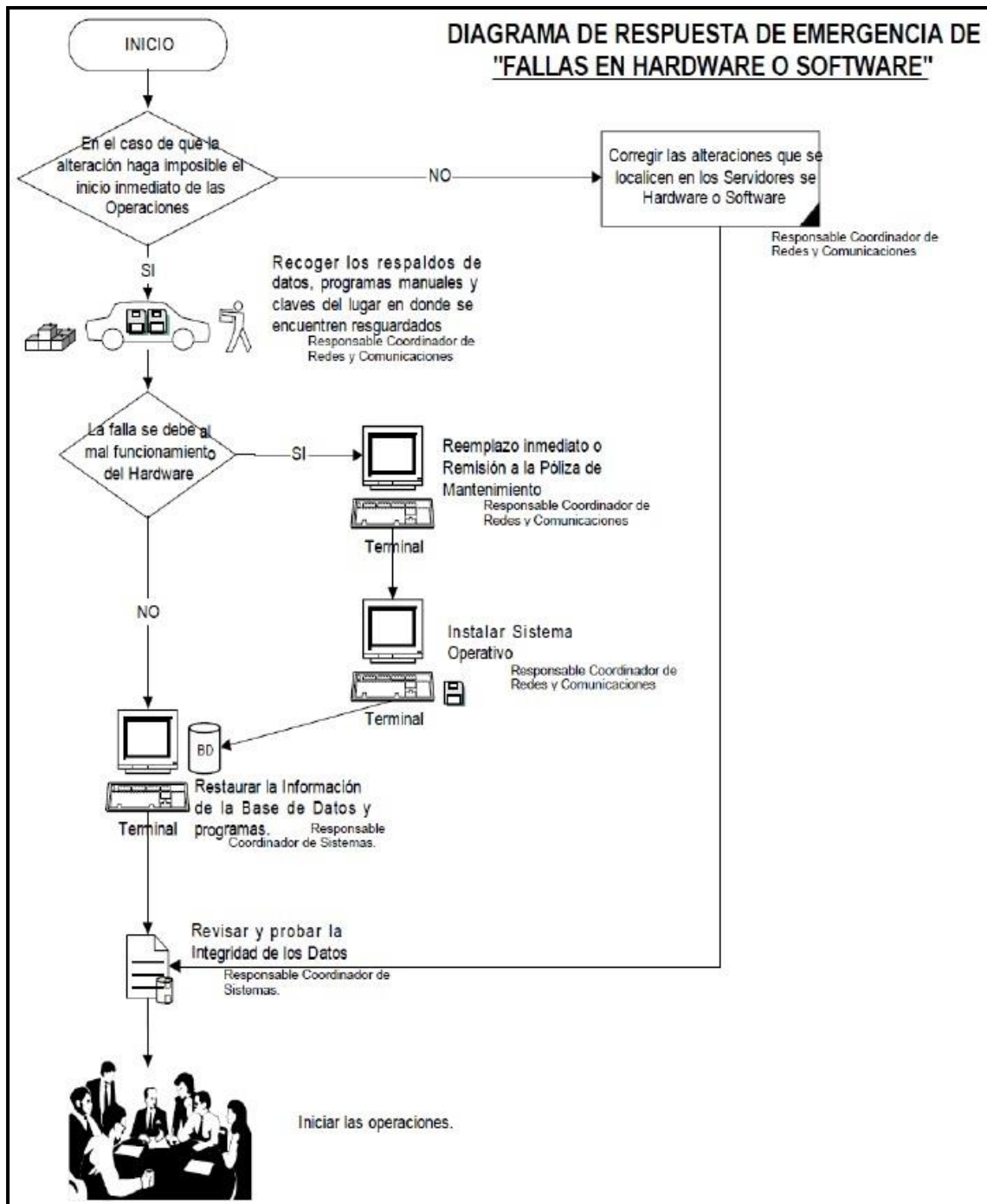


Gráfico N° 06. Plan de contingencia Informático. Delegación Miguel Hidalgo. México, D.F. ArchivoPDF. 2005



## 2.5.4. IMPLEMENTACIÓN PRÁCTICA DE UN PLAN DE CONTINGENCIA.

### MODELO DE DIAGNOSTICO SITUACIONAL.

Actualmente el SIMA Iquitos cuenta con los siguientes Activos Informáticos.

Fuente: Oficina Estratégica SIMA Iquitos S.R.Ltda.

| HARDWARE  | COMUNICACIONES   | SOFTWARE   | DESARROLLO   |
|---|--|--|--|
| <ul style="list-style-type: none"> <li>- 03 UPS.</li> <li>- 79 Computadoras.</li> <li>- 27 Impresoras.</li> <li>- 13 Escáner.</li> <li>- 02 Laptops.</li> </ul> | <ul style="list-style-type: none"> <li>- 08 Switch Administrable.</li> <li>- 02 Router.</li> <li>- 04 Servidores.</li> <li>- 21 Teléfonos IP.</li> </ul> | <ul style="list-style-type: none"> <li>- 43 Office core.</li> <li>- 11 Project.</li> <li>- 09 Autocad LT.</li> <li>- 85 Licencias Antivirus.</li> <li>- 01 Antispan.</li> <li>- 03 Windows Server.</li> <li>- 01 SQL Server.</li> <li>- 01 Microsoft Visual Studio.</li> </ul> | <ul style="list-style-type: none"> <li>- Sistema Contable.</li> <li>- Sistema Financiero.</li> <li>- Sistema de Facturación.</li> <li>- Sistema de Recursos Humanos.</li> <li>- Sistema Comercial.</li> <li>- Sistema de Producción.</li> <li>- Sistema de Cuentas internas 4546.</li> <li>- Sistema de Almacén.</li> <li>- Sistema de inventarios.</li> <li>- Sistema Logístico.</li> </ul> |

### NECESIDAD DE REALIZAR UN MANTENIMIENTO.

Es necesario por tanto la identificación previa de cuales de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

Debe contemplar los planes de emergencia, backup, recuperación, comprobación mediante simulaciones y mantenimiento del mismo. Un plan de contingencia adecuado debe ayudar a las empresas a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio.

### FINALIDAD DE UN PLAN DE CONTINGENCIA.

Tener un Plan de contingencia lo más completo y global posible. Definir las normas y procedimiento necesarios para afrontar cualquier eventualidad



que se produzca en los sistemas de información y comunicación del SIMA Iquitos, de modo que se asegure la continuidad, seguridad y confiabilidad de los mismos.

#### **OBJETIVO GENERAL DE UN PLAN DE CONTINGENCIA.**

Tomar las medidas necesarias para minimizar la probabilidad a los que estará sometido el sistema de información que se va a implementar y, se conviertan en una realidad y posibilitar que el sistema pueda responder sin que ello suponga un grave impacto para su integridad.

#### **OBJETIVOS ESPECÍFICOS DE UN PLAN DE CONTINGENCIA.**

- a. Proteger la vida de las personas inherentes a los servicios informáticos de la entidad.
- b. Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones de la entidad.
- c. Proteger la propiedad de la entidad y otros activos.
- d. Iniciar un procedimiento de recuperación de los servicios informáticos ante un desastre o posibles fallas ocasionadas.
- e. Proteger al sistema de información de pérdidas irreparables de información procesada.
- f. Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los sistemas de información y/o infraestructura informática.
- g. Alcanzar una alta disponibilidad, es decir, impedir que se produzcan fallas en los sistemas, que dificulten el normal funcionamiento de nuestra institución.
- h. Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un sistema de información y/o infraestructura informática.
- i. Impedir que el daño material de cualquier soporte de información, conlleve o no a la pérdida de información: máquinas, instalaciones, líneas de comunicación, etc.; además de otros objetivos como establecer



las medidas organizativas y técnicas para asegurar la confidencialidad, integridad y disponibilidad de la información y el soporte informáticos de nuestra entidad.

#### **2.5.5. POLÍTICAS DE SEGURIDAD FÍSICA.**

##### **ACCESO FÍSICO.**

Las Empresas destinarán un área que servirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y servidores.

Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso al edificio y a las oficinas de Las Empresas.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de tecnología o con permiso de los Administradores TIC.

Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el superior responsable o los Administrador TIC, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del Área Administrativa de Las Empresas y al personal de seguridad del edificio.



## **PROTECCIÓN FÍSICA.**

### **A. Data Center.**

El DataCenter deberá:

1. Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.
2. Ser un área restringida. Tener un sistema de control de acceso que garantice solo la entrada al personal autorizado por la Gerencia o Jefatura de TI.
3. Aire acondicionado. Mantener la temperatura a 17° C. de ser posible contar un aire acondicionado de precisión que cuente con un sistema de control deshumecedor para mayor control de la temperatura.
4. Respaldo de energía redundante. Contar con equipos UPS con autonomía mínima de 1 hora. Además de contar con un sistema electrógeno propio.
5. Seguir los estándares de protección eléctrica vigentes para minimizar los riesgos de daños físicos de los equipos de telecomunicaciones y servidores.
6. Los sistemas de tierra física, sistema de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
7. Contar con algún esquema que asegure la continuidad del servicio.
8. Control de humedad.
9. Prevención y/o detección de incendios.
10. Sistema de extinción.

### **B. Infraestructura.**

Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.



El resguardo de los equipos de cómputo deberá quedar bajo el área de Tecnología contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

#### 2.5.6. NIVELES DE SEGURIDAD

El departamento de Defensa de los Estados Unidos ha definido unos niveles de seguridad para sus computadoras, que se recogen en el denominado “Libro Naranja” (por el color de sus tapas), y que es usado como un estándar para indicar el nivel de seguridad de los sistemas informáticos.

Estas especificaciones definen siete niveles de seguridad, denominadas A1, B3, B2, B1, C2, C1, D. Siendo el D de menor seguridad y A1 de mayor. Cada nivel incluye las exigencias de los niveles inferiores.

**Nivel D.** Estos sistemas tienen exigencias de seguridad mínimos, no se les exige nada en particular para ser considerados de clase D.

**Nivel C1.** Para que un sistema sea considerado C1 tiene que permitir la separación entre datos y usuarios, debe permitirse a un usuario limitar el acceso a determinados datos, y los usuarios tiene que identificarse y validarse para ser admitidos en el sistema.

**Nivel C2.** Para que un sistema sea de tipo C2 los usuarios tiene que poder admitir o denegar el acceso a datos a usuarios en concreto, debe de llegar una auditoria de accesos, e intentos fallidos de acceso a objetos (archivos, etc.), y también especifica que los procesos no dejen residuos.

**Nivel B1.** A un sistema de nivel B1 se le exige control de acceso obligatorio, cada objeto del sistema (usuario o dato) se le asigna una etiqueta, con un nivel de seguridad jerárquico y con unas categorías.

**Nivel B2.** Un sistema de nivel B2 debe tener un modelo teórico de seguridad verificable, ha de existir un usuario con los privilegios necesarios para implementar las políticas de control, y este usuario tiene que ser distinto del administrador del sistema. Los canales de



entrada y salida de datos tienen que estar restringidos para evitar fugas de datos o la instrucción de estos.

**Nivel B3.** En el nivel B3 tiene que existir un argumento convincente de que el sistema es seguro, ha de poderse definir la protección para cada objeto, objetos permitidos y cuáles no, y el nivel de acceso permitido a cada cual. Tiene que existir un monitor de referencia que reciba las peticiones de acceso de cada usuario y las permita o las deniegue según las políticas de acceso que se hayan definido. El sistema debe ser muy resistente a la penetración de intrusos, así como tener una auditoria que permita detectar posibles violaciones de la seguridad.

**Nivel A1.** Los sistemas de nivel A1 deben cumplir los mismos requerimientos que los de nivel B3, pero debe ser comprobado formalmente el modelo de seguridad definido en el nivel B3.

## 2.6. ETAPAS PARA IMPLEMENTAR UN SISTEMA DE SEGURIDAD

Para implementar un Sistema de Seguridad, y los elementos que componen este sistema empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguientes 8 pasos:

1. Introducir el tema de seguridad en la visión de la empresa.
2. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
3. Capacitar al gerente y directivos, contemplando el enfoque global.
4. Designar y capacitar supervisores de área.
5. Definir trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
6. Mejorar las comunicaciones internas.
7. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
8. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.



### 2.6.1. ANÁLISIS DE RIESGO.

Cuando usted crea una política de seguridad de red, es importante que comprenda que la razón para crear una política es, en primer lugar, asegurar que los esfuerzos dedicados a la seguridad impliquen un costo razonable. Esto significa que usted debe conocer cuales recursos vale la pena proteger, y cuales son más importantes que otros. También debe identificar la fuente de amenazas de la que usted está protegiendo a los recursos de la red. A pesar de toda la publicidad acerca de los intrusos que irrumpen en una red, muchos estudios indican que, en el caso de la mayoría de las organizaciones, las verdaderas pérdidas causadas por los usuarios internos son mucho mayores.

El análisis de riesgo implica determinar lo siguiente:

- ✓ **¿Qué necesita proteger?**
- ✓ **¿De qué necesita protegerlo?**
- ✓ **¿Cómo protegerlo?**

Los riesgos deben clasificarse por nivel de importancia y gravedad de la pérdida. No debe terminar en una situación en la que gaste más en proteger algo que es de menor valor para usted.

La evaluación de la amenaza y los riesgos no debe ser una actividad de una sola vez; debe realizarse con regularidad, como se defina en la política de seguridad del sitio.

Otros factores que hay que considerar al estimar el riesgo de un recurso de red son su disponibilidad, integridad y confidencialidad. La disponibilidad de un recurso es la medida de qué tan importante es tenerlo disponible todo el tiempo. La integridad de un recurso es la medida de que tan importante es que este o los datos del mismo sean consistentes.

Esto es de particular importancia para los recursos de bases de datos. La confidencialidad se aplica a recursos, tales como archivos de datos, a los cuales se desee restringir el acceso.

### 2.6.2. IDENTIFICACIÓN DE RECURSOS



Al realizar el análisis de riesgo, usted debe identificar todos los recursos que corran el riesgo de sufrir una violación de seguridad. Los recursos como el hardware son bastante obvios para incluirlos en este cálculo, pero en muchas ocasiones se ignoran recursos tales como las personas que en realidad utilizan los sistemas. Es importante identificar a todos los recursos de la red que puedan ser afectados por un problema de seguridad.

La RFC 1244 enlista los siguientes recursos de red que usted debe considerar al calcular las amenazas a la seguridad general:

1. **HARDWARE:** procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadores personales, impresoras, unidades de disco, líneas de comunicación, servidores terminales, routers.
2. **SOFTWARE:** programas fuente, programas objeto, utileras, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
3. **DATOS:** durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoría, base de datos, en tránsito a través de medios de comunicación.
4. **PERSONAS:** usuarios, personas necesarias para operar los sistemas.
5. **DOCUMENTACIÓN:** sobre programas, hardware, sistemas, procedimientos administrativos locales.
6. **SUMINISTROS:** papel, formularios, medios magnéticos.

### 2.6.3. IDENTIFICACIÓN DE LAS AMENAZAS

Una vez que se han identificado los recursos que requieren protección, usted debe identificar las amenazas a las que están expuestos. Pueden examinarse las amenazas para determinar qué posibilidad de pérdida existe. También debe identificar de qué amenazas está usted tratando de proteger a sus recursos.



#### **2.6.4. RIESGO DE REVELACIÓN DE INFORMACIÓN**

La revelación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Usted debe determinar el valor y delicadeza de la información guardada en sus computadoras. En el caso de vendedores de hardware y software, el código fuente, los detalles de diseño, los diagramas y la información específica de un producto representan una ventaja competitiva.

Los hospitales, las compañías de seguros y las instituciones financieras mantienen información confidencial, cuya revelación puede ser perjudicial para los clientes y la reputación de la empresa. Los laboratorios farmacéuticos pueden tener aplicaciones patentadas y no pueden arriesgarse a pérdidas causadas por robos.

A nivel del sistema, la revelación de un archivo de contraseñas de un sistema Unix puede volverlo vulnerable a accesos no autorizados en el futuro. Para muchas organizaciones, un vistazo, a una propuesta o un proyecto de investigación que represente muchos años de trabajo puede darle a su competidor una ventaja injusta.

Muchas veces, la gente supone que los accesos no autorizados de terceros a las redes y computadoras son realizadas por individuos que trabajan por su cuenta. No siempre es así. Los peligros del espionaje industrial gubernamental sistemático son realidades desafortunadas de la vida.

Además, cuando se logra uno de estos accesos no autorizados, por lo general la información fluye por Internet en muy poco tiempo. Hay grupos de noticias y canales de difusión, en Internet (IRC) en los que los usuarios comparten la información que lograron extraer de estas intromisiones.

#### **2.7. AUDITORÍA DE SISTEMAS**



La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

### **2.7.1. PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA.**

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

- ✓ Evaluación de los sistemas y procedimientos.
- ✓ Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de



informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

### **2.7.2. CONTROL DE PROYECTOS.**

Debido a las características propias del análisis y la programación, es muy frecuente que la implantación de los sistemas se retrase y se llegue a suceder que una persona lleva trabajando varios años dentro de un sistema o bien que se presenten irregularidades en las que los programadores se ponen a realizar actividades ajenas a la dirección de informática.

Para poder controlar el avance de los sistemas, ya que ésta es una actividad de difícil evaluación, se recomienda que se utilice la técnica de administración por proyectos para su adecuado control.

Para tener una buena administración por proyectos se requiere que el analista o el programador y su jefe inmediato elaboren un plan de trabajo en el cual se especifiquen actividades, metas, personal participante y tiempos. Este plan debe ser revisado periódicamente (semanal, mensual, etc.) para evaluar el avance respecto a lo programado.

La estructura estándar de la planeación de proyectos deberá incluir la facilidad de asignar fechas predefinidas de terminación de cada tarea. Dentro de estas fechas debe estar el calendario de reuniones de revisión, las cuales tendrán diferentes niveles de detalle.

### **2.7.3. CONTROLES.**



Los datos son uno de los recursos más valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

- a. La responsabilidad de los datos es compartida conjuntamente por alguna función determinada y el departamento de cómputo.
- b. Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.
- c. Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.
- d. Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

### **CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO**

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que servirán de base a registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas o discos magnéticos y ópticos.



Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de procesos.

### **CONTROL DE MANTENIMIENTO.**

Como se sabe existen básicamente tres tipos de contrato de mantenimiento: El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes. El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento es “por llamada”, en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo (casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como “en banco”, y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura más las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe primero analizar cuál de los tres tipos es el que más nos conviene y en segundo lugar pedir los contratos y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.



## **2.8. SEGURIDAD EN CENTROS DE CÓMPUTO**

### **2.8.1. ORDEN EN EL CENTRO DE CÓMPUTO.**

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del sistema de cómputo, los discos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

### **2.8.2. SEGURIDAD LÓGICA Y CONFIDENCIAL**

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Antes esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado "virus" de las computadoras, el cual aunque tiene diferentes intenciones se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.



El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos. Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

### **2.8.3. SEGURIDAD FÍSICA.**

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.

Entre las precauciones que se deben revisar están:

- ✓ Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.
- ✓ En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
- ✓ En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede



sucedir que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.

- ✓ Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.
- ✓ Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.
- ✓ También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
- ✓ Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.
- ✓ Los materiales más peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

#### **2.8.4. SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO.**

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

1. Se debe restringir el acceso a los programas y a los archivos.
2. Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
3. Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
4. No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
5. Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.



6. Se deben monitorear periódicamente el uso que se le está dando a las terminales.
7. Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.
8. El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.
9. Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.
10. Debe controlarse la distribución de las salidas (reportes, cintas, etc.).
11. Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.
12. Se debe tener un estricto control sobre el acceso físico a los archivos.
13. En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que nos signifiquen nada y que sean difíciles de identificar, lo que evitará que el programador utilice la computadora para trabajos personales. Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Para controlar este tipo de información se debe:

- 1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.
- 2) Sólo el personal autorizado debe tener acceso a la información confidencial.
- 3) Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.



- 4) Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

- ✓ Equipo, programas y archivos
- ✓ Control de aplicaciones por terminal
- ✓ Definir una estrategia de seguridad de la red y de respaldos
- ✓ Requerimientos físicos.
- ✓ Estándar de archivos.
- ✓ Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

#### **2.8.5. PROCEDIMIENTO DE RESPALDO EN CASO DE DESASTRE**

Se debe establecer en cada dirección de informática un plan de emergencia el cual ha de ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia, se tenga la seguridad que funcionará.

La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se ha de utilizar respaldos.

Se deben evitar suposiciones que, en un momento de emergencia, hagan inoperante el respaldo, en efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo, en disco etc.



El plan de emergencia una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.

En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia, La estructura del plan debe ser tal que facilite su actualización.

Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática, debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa.

Los desastres que pueden suceder podemos clasificar así:

- a. Completa destrucción del centro de cómputo,
- b. Destrucción parcial del centro de cómputo,
- c. Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado, etc.)
  - a. Destrucción parcial o total de los equipos descentralizados
  - b. Pérdida total o parcial de información, manuales o documentación
  - c. Pérdida del personal clave
  - d. Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

- ✓ La documentación de programación y de operación.
- ✓ Los equipos:
  - El equipo completo
  - El ambiente de los equipos
  - Datos y archivos



- Papelería y equipo accesorio
- Sistemas (sistemas operativos, bases de datos, programas).

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá:

- ✓ Asegurarse de que todos los miembros sean notificados,
- ✓ Informar al director de informática,
- ✓ Cuantificar el daño o pérdida del equipo, archivos y documentos para definir qué parte del plan debe ser activada.
- ✓ Determinar el estado de todos los sistemas en proceso,
- ✓ Notificar a los proveedores del equipo cual fue el daño,
- ✓ Establecer la estrategia para llevar a cabo las operaciones de emergencias tomando en cuenta:
  - Elaboración de una lista con los métodos disponibles para realizar la recuperación.
  - Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustituciones de procesos en línea por procesos en lote).
  - Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.
  - Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deberá reducir la carga de procesos, analizando alternativas como:

- ✓ Posponer las aplicaciones de prioridad más baja,
- ✓ Cambiar la frecuencia del proceso de trabajos.
- ✓ Suspender las aplicaciones en desarrollo.



Por otro lado, se debe establecer una coordinación estrecha con el personal de seguridad a fin de proteger la información.

Respecto a la configuración del equipo hay que tener toda la información correspondiente al hardware y software del equipo propio y del respaldo. Deberán tenerse todas las especificaciones de los servicios auxiliares tales como energía eléctrica, aire acondicionado, etc. a fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de procesos, se deberán tomar en cuenta las siguientes consideraciones:

- ✓ Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.
- ✓ Se debe tener documentados los cambios de software.
- ✓ En caso de respaldo en otras instituciones, previamente se deberá conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

- ✓ Configuración de equipos.
- ✓ Configuración de equipos de captación de datos.
- ✓ Sistemas operativos.
- ✓ Configuración de equipos periféricos.



### III. CONCLUSIONES

- ✓ Se describieron las políticas, la planeación y el análisis de riesgo de la seguridad en redes, mostrando aspectos como la importancia de las TIC's para el continuo desarrollo y sostenibilidad de la organización.
- ✓ Se debe de realizar un análisis para establecer la vulnerabilidad de la información valiosa para la organización, además de identificar las posibles vulnerabilidades.
- ✓ Se logró identificar los parámetros para para el diseño de la política de red.
- ✓ La auditoría en la organización es un elemento de control que permite llevar la revisión y evaluación de los controles, sistemas y procedimientos de informática. Además de que es de vital importancia para el buen desempeño de los sistemas de información.



#### IV. RECOMENDACIONES

- ✓ APLICAR UNA CORRECTA PLANEACIÓN DE SEGURIDAD EN REDES PERMITE TENER UN CAMPO DE CONTROL MAYOR, ESTO SE DEBE EJECUTAR EN LAS ORGANIZACIONES PARA DISMINUIR EN LO POSIBLE LAS VULNERABILIDADES QUE PUDIERAN EXISTIR Y SER PROVOCADOS POR FALLAS EN EL PROCESO DE PLANEAMIENTO.
- ✓ PARA GARANTIZAR LA PRIVACIDAD DE LA INFORMACIÓN Y LA CONTINUIDAD DE LOS SERVICIOS TIC ES NECESARIO TOMAR EN CUENTA LA IMPORTANCIA DE SEGURIDAD DE LA INFORMACIÓN, YA QUE ESTA PRETENDE EN LO POSIBLE DE MINIMIZAR LOS RIEGOS Y/O VULNERABILIDADES DE LOS SISTEMAS Y DE LA INFORMACIÓN CONTENIDA EN ELLA.
- ✓ SE RECOMIENDA QUE EL ESTADO COMO ENTE REGULADOR DE LAS TELECOMUNICACIONES DEBE DE ENFATIZAR LA CIBERSEGURIDAD COMO PLAN DE ESTADO, CUYO OBJETO ES LA PROTECCIÓN DE LAS ORGANIZACIONES Y LAS INSTITUCIONES CONTRA LOS ATAQUES QUE LOS CIBERCRIMINALES LANZAN PARA COMPROMETER SUS SISTEMAS DE INFORMACIÓN DE HARDWARE Y DE SOFTWARE Y CONTRA EL ROBO DE INFORMACIÓN QUE ALMACENAN.
- ✓ POR OTRA PARTE, SE RECOMIENDA QUE LAS ORGANIZACIONES TOMEN MEDIDAS DE PROTECCIÓN REFERENTES A LA CIBERSEGURIDAD Y LA PROTECCIÓN DE LOS SISTEMAS INFORMÁTICOS.
- ✓ SE RECOMIENDA QUE LAS ORGANIZACIONES E INSTITUCIONES DEBAN DE IMPLEMENTAR POLITICAS DE SEGURIDAD TIC QUE PERMITAN CONTROLAR O MITIGAR LOS RIESGOS DE ATAQUES Y/O ERRORES (BUGS) DE LOS SISTEMAS INFORMATICOS A NIVEL DE HARDWARE Y SOFTWARE; POR CONSIGUIENTE TAMBIÉN SE DEBE DE IMPLEMENTAR NORMATIVAS QUE APLIQUEN LAS POLITICAS IMPLEMENTADAS.
- ✓ LA GESTIÓN DE LOS SERVICIOS INFORMÁTICOS Y DE GOBIERNO TI SE EVALÚAN CON UN CONJUNTO DE HERRAMIENTAS QUE PERMITEN UNA BUENA PRÁCTICA PARA EL CONTROL DE LA INFORMACIÓN, TIC Y LOS RIESGOS QUE ESTOS CONLLEVAN; PARA ESTO SE RECOMIENDA QUE LAS ORGANIZACIONES IMPLEMENTEN ESTÁNDARAS INTERNACIONALES DE BUENAS PRÁCTICAS COMO POR EJEMPLO (COBIT, ITIL, ETC).



## V. REFERENCIA BIBLIOGRÁFICA

- ✓ LUIS DANIEL ALVAREZ BASUALDA, SEGURIDAD INFORMÁTICA, MEXICO, 2005.
- ✓ ING. MARÍA VICTORIA BAJARLÍA, MODELO DEL CONOCIMIENTO EN SEGURIDAD DE APLICACIONES, BUENOS AIRES, 2010.
- ✓ ESTADO DE LA CIBERSEGURIDAD 2015, CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL, DISPONIBLE EN:  
<http://globbsecurity.com/download/36615/>
- ✓ GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA, BLOG DE WORDPRESS, DISPONIBLE EN:  
[https://protejete.wordpress.com/gdr\\_principal/amenazas\\_vulnerabilidades/](https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/)
- ✓ POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, 10 DE OCTUBRE DEL 2013, DISPONIBLE EN:  
<http://www.segu-info.com.ar/politicas/polseginf.htm>
- ✓ JORGE BURGOS SALAZAR, PEDRO G. CAMPOS, UNIVERSIDAD DEL BÍO-BÍO, MODELOS PARA SEGURIDAD DE LA INFORMACIÓN EN TIC, CHILE, 2013  
DISPONIBLE EN:  
<http://ceur-ws.org/Vol-488/paper13.pdf>