CAPÍTULO 9

"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más... Más vale dedicar recursos a la seguridad que convertirse en una estadística."

POLÍTICAS DE SEGURIDAD

Hoy es imposible hablar de un sistema cien por cien seguro, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. "Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares".

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un

conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

9.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Está lejos de mi intención (y del alcance del presente) proponer un documento estableciendo lo que debe hacer un usuario o una organización para lograr la mayor Seguridad Informática posible. Sí está dentro de mis objetivos proponer los lineamientos generales que se deben seguir para lograr (si así se pretendiese) un documento con estas características.

El presente es el resultado de la investigación, pero sobre todo de mi experiencia viendo como muchos documentos son ignorados por contener planes y políticas difíciles de lograr, o peor aún, de entender.

Esto adquiere mayor importancia aún cuando el tema abordado por estas políticas es la Seguridad Informática. Extensos manuales explicando como debe protegerse una computadora o una red con un simple Firewall, un programa antivirus o un monitor de sucesos. Falacias altamente remuneradas que ofrecen la mayor "Protección" = "Aceite de Serpiente" del mundo.

He intentado dejar en claro que la Seguridad Informática no tiene una solución definitiva aquí y ahora, sino que es y será (a mi entender) el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables de nuestros sistemas.

En palabras de Julio C. Ardita: "Una política de seguridad funciona muy bien en EE.UU. pero cuando estos manuales se trajeron a América Latina fue un fiasco... Armar una política de procedimientos de seguridad en una empresa está costando entre 150–350 mil dólares y el resultado es ninguno... Es un manual que llevado a la implementación nunca se realiza... Es muy difícil armar algo global, por lo que siempre se trabaja en un plan de seguridad real: las políticas y procedimientos por un lado y la parte física por otra."[1]

[1] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. *http://www.cybsec.com*

Para continuar, hará falta definir algunos conceptos aplicados en la definición de una PSI:

Decisión: elección de un curso de acción determinado entre varios posibles.

Plan: conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.

Estrategia: conjunto de decisiones que se toman para determinar políticas, metas y programas.

Política: definiciones establecidas por la dirección, que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

Meta: objetivo cuantificado a valores predeterminados.

Procedimiento: Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.

Norma: forma en que realiza un procedimiento o proceso.

Programa: Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.

Proyección: predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.

Pronostico: predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirán en los acontecimientos futuros.

Control: capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.[2]

Riesgo: proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

Ahora, "una **Política de Seguridad** es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema."[3]

La RFC 1244 define **Política de Seguridad** como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán."[4]

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, "(...) una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas."[5] y debe:

[2] FERNADEZ, Carlos M. Seguridad en sistemas informáticos. Ediciones Díaz de Santos S.A.. España. 1988. Página 105.

[3] HUERTA, Antonio Villalón. Seguridad en Unix y redes. (Versión 1.2). Capítulo 16–Página 259

[4] RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991

[5] SPAFFORD, Gene. "Manual de seguridad en redes". ArCERT. Argentina. 2000. *http://www.arcert.gov.ar*

- Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Cualquier política de seguridad ha de contemplar los elementos claves de seguridad ya mencionados: la Integridad, Disponibilidad, Privacidad y, adicionalmente, Control, Autenticidad y Utilidad.

No debe tratarse de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el porqué de ello.

9.2 EVALUACIÓN DE RIESGOS

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas.

- Se debe poder obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir).
- Se debe tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.
- Se debe conocer qué se quiere proteger, dónde y cómo, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos (hardware, software, información, personal, accesorios, etc.) con que se cuenta y las amenazas a las que se está expuesto.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización; pero se puede presupone algunas preguntas que ayudan en la identificación de lo anteriormente expuesto[6]:

- "¿Qué puede ir mal?"
- "¿Con qué frecuencia puede ocurrir?"
- "¿Cuáles serían sus consecuencias?"
- "¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?"
- "¿Se está preparado para abrir las puertas del negocio sin sistemas, por un día, una semana, cuanto tiempo?"

[6] RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991

- "¿Cuál es el costo de una hora sin procesar, un día, una semana...?"
- "¿Cuánto, tiempo se puede estar off–line sin que los clientes se vayan a la competencia?"
- "¿Se tiene forma de detectar a un empleado deshonesto en el sistema?"
- "¿Se tiene control sobre las operaciones de los distintos sistemas?"
- "¿Cuantas personas dentro de la empresa, (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?"
- "¿A que se llama información confidencial y/o sensitiva?"
- "¿La información confidencial y sensitiva permanece así en los sistemas?"
- "¿La seguridad actual cubre los tipos de ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?"
- "¿A quien se le permite usar que recurso?"
- "¿Quién es el propietario del recurso? y ¿quién es el usuario con mayores privilegios sobre ese recurso?"
- "¿Cuáles serán los privilegios y responsabilidades del Administrador vs. la del usuario?"
- "¿Cómo se actuará si la seguridad es violada?"

Una vez obtenida la lista de cada uno de los riesgos se efectuará un resumen del tipo:

Tipo de Riesgo	Factor
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Tabla 9.1 – Tipo de Riesgo–Factor

Según esta tabla habrá que tomar las medidas pertinentes de seguridad para cada caso en particular, cuidando incurrir en los costos necesarios según el factor de riesgo representado.

9.2.1 NIVELES DE RIESGO

Como puede apreciarse en la Tabla 9.1, los riesgos se clasifican por su nivel de importancia y por la severidad de su pérdida:

1. Estimación del riesgo de pérdida del recurso (R_i)
2. Estimación de la importancia del recurso (I_i)

Para la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico de 0 a 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).

El riesgo de un recurso será el producto de su importancia por el riesgo de perderlo[7]:

$$WR_i = R_i * I_i$$

Luego, con la siguiente fórmula es posible calcular el riesgo general de los recursos de la red:

$$W_R = \frac{(WR_1 * I_1 + WR_2 * I_2 + ... + WR_n * I_n)}{I_1 + I_2 + ... + I_n}$$

Otros factores que debe considerar para el análisis de riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial, los cuales pueden incorporarse a la fórmula para ser evaluados.

Ejemplo: el Administrador de una red ha estimado los siguientes riesgos y su importancia para los elementos de la red que administra:

Recurso	Riesgo (R_i)	Importancia (I_i)	Riesgo Evaluado (R_i*I_i)
Router	6	7	42
Gateway	6	5	30
Servidor	10	10	100
PC's	9	2	18

Tabla 9.2 – Valuación de Riesgos

Aquí ya puede apreciarse que el recurso que más debe protegerse es el servidor. Para la obtención del riesgo total de la red calculamos:

$$W_R = \frac{42 + 30 + 100 + 18}{7 + 5 + 10 + 2} = 7{,}92$$

Al ver que el riesgo total de la red es de casi 8 puntos sobre 10 debería pensarse seriamente en buscar las probables causas que pueden provocar problemas a los servicios brindados por los elementos evaluados.

9.2.2 IDENTIFICACIÓN DE AMENAZA

Una vez conocidos los riesgos, los recursos que se deben proteger y como su daño o falta pueden influir en la organización es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos. Como ya se mencionó existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe la otra tampoco.

Se suele dividir las amenazas existentes según su ámbito de acción:

- Desastre del entorno (Seguridad Física).
- Amenazas del sistema (Seguridad Lógica).
- Amenazas en la red (Comunicaciones).
- Amenazas de personas (Insiders–Outsiders).

[7] "Manual de seguridad en redes". ArCERT. Argentina. 2000. Página 3–1. *http://www.arcert.gov.ar*

Se debería disponer de una lista de amenazas (actualizadas) para ayudar a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar. Es importante que los Administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

En la siguiente sección se explica una metodología para definir una estrategia de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales.

La metodología se basa en los distintos ejemplos (uno para cada tipo de amenaza) y contempla como hubiera ayudado una política de seguridad en caso de haber existido.

9.2.3 EVALUACIÓN DE COSTOS

Desde un punto de vista oficial, el desafío de responder la pregunta del valor de la información ha sido siempre difícil, y más difícil aún hacer estos costos justificables, siguiendo el principio que "si desea justificarlo, debe darle un valor"[8].

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea. Por eso es importante entender que los esfuerzos invertidos en la seguridad son costeables.

La evaluación de costos más ampliamente aceptada consiste en cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades. Un planteamiento posible para desarrollar esta política es el análisis de lo siguiente:

- ¿Qué recursos se quieren proteger?
- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

Con esas sencillas preguntas (más la evaluación de riesgo) se debería conocer cuáles recursos vale la pena (y justifican su costo) proteger, y entender que algunos son más importantes que otros.

El objetivo que se persigue es lograr que un ataque a los bienes sea más costoso que su valor, invirtiendo menos de lo que vale. Para esto se define tres costos fundamentales:

[8] STRASSMANN, Paul A. "El arte de presupuestar: como justificar los fondos para Seguridad Informática". *http://www.nextvision.com*

- **CP:** Valor de los bienes y recursos protegidos.
- **CR:** Costo de los medios necesarios para romper las medidas de seguridad establecidas.
- **CS:** Costo de las medidas de seguridad.

Para que la política de seguridad sea lógica y consistente se debe cumplir que:

- **CR > CP**: o sea que un ataque para obtener los bienes debe ser más costoso que el valor de los mismos. Los beneficios obtenidos de romper las medidas de seguridad no deben compensar el costo de desarrollo del ataque.
- **CP > CS:** o sea que el costo de los bienes protegidos debe ser mayor que el costo de la protección.

Luego, **CR > CP > CS** y lo que se busca es:

- "**Minimizar** el costo de la protección manteniéndolo por debajo del de los bienes protegidos"[9]. Si proteger los bienes es más caro de lo que valen (el lápiz dentro de la caja fuerte), entonces resulta más conveniente obtenerlos de nuevo en vez de protegerlo.
- "**Maximizar** el costo de los ataques manteniéndolo por encima del de los bienes protegidos"[10]. Si atacar el bien es más caro de lo que valen, al atacante le conviene más obtenerlo de otra forma menos costosa.

Se debe tratar de valorar los costos en que se puede incurrir en el peor de los casos contrastando con el costo de las medidas de seguridad adoptadas. Se debe poner especial énfasis en esta etapa para no incurrir en el error de no considerar costos, muchas veces, ocultos y no obvios (costos derivados).

9.2.3.1 VALOR INTRÍNSECO

Es el más fácil de calcular (pero no fácil) ya que solo consiste en otorgar un valor a la información contestando preguntas como las mencionadas y examinando minuciosamente todos los componentes a proteger.

9.2.3.2 COSTOS DERIVADOS DE LA PERDIDA

Una vez más deben abarcarse todas las posibilidades, intentando descubrir todos los valores derivados de la pérdida de algún componente del sistema. Muchas veces se trata del valor añadido que gana un atacante y la repercusión de esa ganancia para el entorno, además del costo del elemento perdido. Deben considerarse elementos como:

- Información aparentemente inocua como datos personales, que pueden permitir a alguien suplantar identidades.

[9] POYATO, Chelo–COLL, Francisco–MORENO David. Definición de una política de seguridad. España. 2000. *http://www.rediris.es/cert*

[10] RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991

- Datos confidenciales de acuerdos y contratos que un atacante podría usar para su beneficio.
- Tiempos necesarios para obtener ciertos bienes. Un atacante podría acceder a ellos para ahorrarse el costo (y tiempo) necesario para su desarrollo.

9.2.3.3 PUNTO DE EQUILIBRIO

Una vez evaluados los riesgos y los costos en los que se está dispuesto a incurrir y decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio entres estas magnitudes:

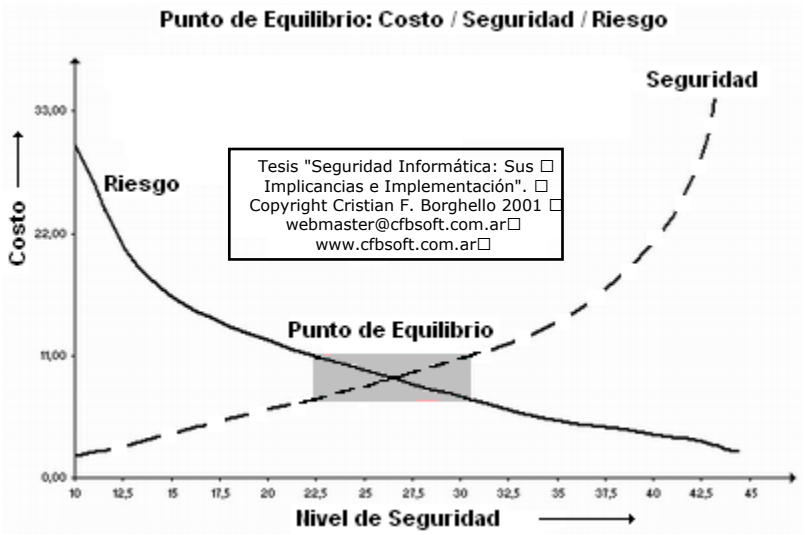

Gráfico 9.1 – Punto de equilibrio Costo/Seguridad

Como puede apreciarse los riesgos disminuyen al aumentar la seguridad (y los costos en los que incurre) pero como ya se sabe los costos tenderán al infinito sin lograr el 100% de seguridad y por supuesto nunca se logrará no correr algún tipo de riesgo. Lo importante es lograr conocer cuan seguro se estará conociendo los costos y los riesgos que se corren (Punto de Equilibrio).

9.3 ESTRATEGIA DE SEGURIDAD

Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles que esta debe abarcar y que no son ni mas ni menos que los estudiados hasta aquí: Física, Lógica, Humana y la interacción que existe entre estos factores.

En cada caso considerado, el plan de seguridad debe incluir una estrategia Proactiva y otra Reactiva[11].

La **Estrategia Proactiva** (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes

[11] BENSON, Christopher. Estrategias de Seguridad. Inobis Consulting Pty Ltd. Microsoft© Solutions. *http://www.microsoft.com/latam/technet/articulos/200011*

en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

La **Estrategia Reactiva** (perseguir y procesar) o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- **Lo que no se permite expresamente está prohibido**: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.
- **Lo que no se prohíbe expresamente está permitido**: significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no.

Actualmente, y "gracias" a las, cada día más repetitivas y eficaces, acciones que atentan contra los sistemas informáticos los expertos se inclinan por recomendar la primera política mencionada.

9.3.1 IMPLEMENTACIÓN

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 informática 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 porque 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:

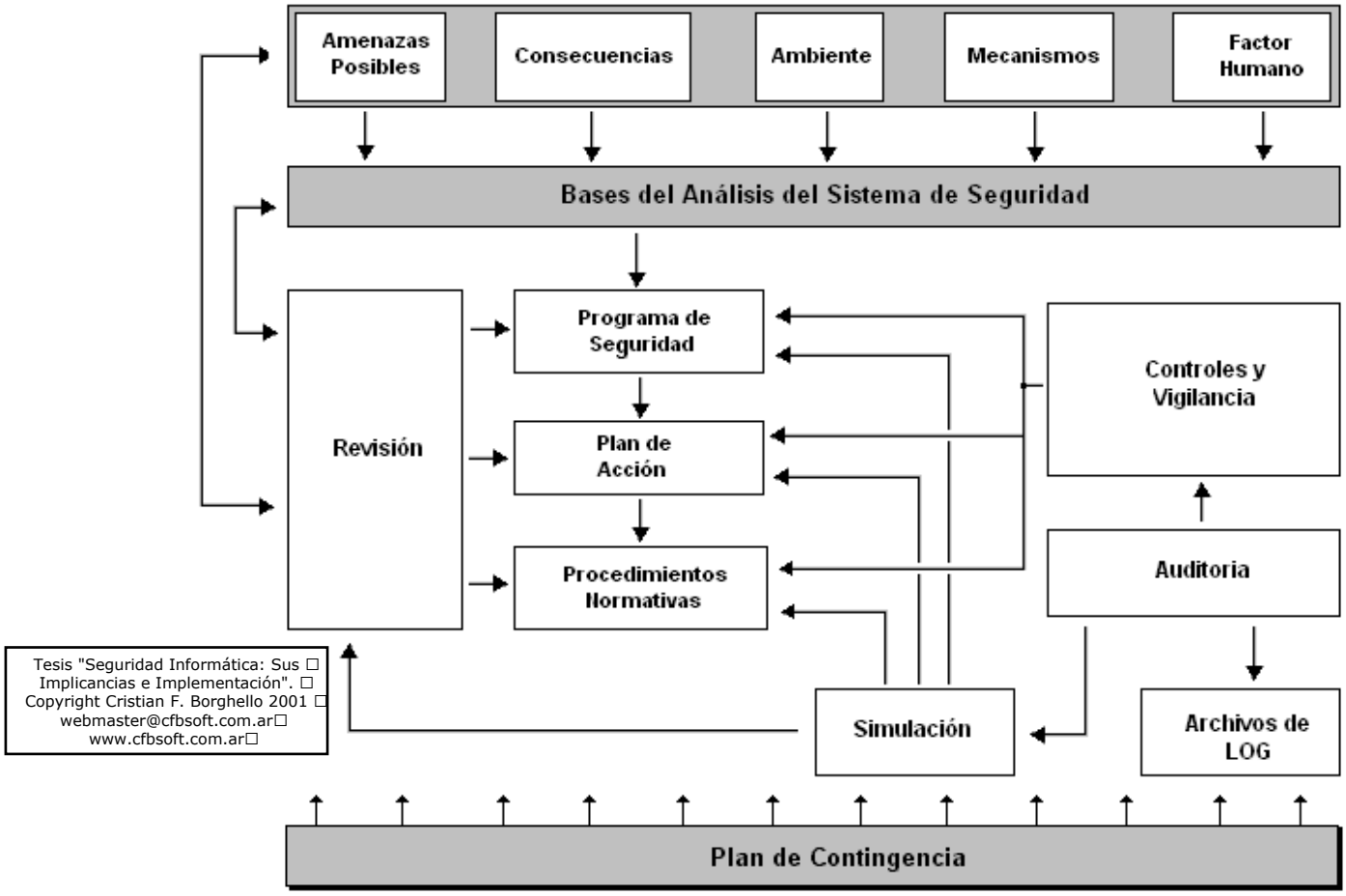

Gráfico 9.2 – Fuente: Manual de Seguridad en Redes. *http://www.arcert.gov.ar*

Se comienza realizando una evaluación del factor humano, el medio en donde se desempeña, los mecanismos con los cuales se cuenta para llevar a cabo la tarea encomendada, las amenazas posibles y sus posibles consecuencias.

Luego de evaluar estos elementos y establecida la base del análisis, se originan un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

Para que todo lo anterior llegue a buen fin debe realizarse un control periódico de estas políticas, que asegure el fiel cumplimiento de todos los procedimientos enumerados. Para asegurar un marco efectivo se realiza una auditoría a los archivos Logs de estos controles.

Con el objeto de confirmar que todo lo creado funciona en un marco real, se realiza una simulación de eventos y acontecimientos que atenten contra la seguridad del sistema. Esta simulación y los casos reales registrados generan una realimentación y revisión que permiten adecuar las políticas generadas en primera instancia.

Por último el Plan de Contingencia es el encargado de suministrar el respaldo necesario en caso en que la política falle.

Es importante destacar que la Seguridad debe ser considerada desde la fase de diseño de un sistema. Si la seguridad es contemplada luego de la implementación del mismo, el personal se enfrentará con problemas técnicos, humanos y administrativos muchos mayores

que implicaran mayores costos para lograr, en la mayoría de los casos, un menor grado de seguridad.

"Construya la seguridad desde el principio. La máxima de que es más caro añadir después de la implementación es cierta."[12]

Julio C. Ardita menciona: "Muchas veces nos llaman cuando está todo listo, faltan dos semanas y quieren que lo aseguremos (...) llegamos, miramos y vemos que la seguridad es imposible de implementar. Últimamente nos llaman en el diseño y nosotros los orientamos y proponemos las soluciones que se pueden adoptar (...)"[13]

Queda claro que este proceso es dinámico y continuo, sobre el que hay que adecuarse continuamente a fin de subsanar inmediatamente cualquier debilidad descubierta, con el fin de que estas políticas no caigan en desuso.

9.3.2 AUDITORÍA Y CONTROL

Se considera que la Auditoría son los "ojos y oídos" de la dirección, que generalmente no puede, no sabe o no debe realizar las verificaciones y evaluaciones.

La Auditoría consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno y cuando lo hace.

En cuanto al objetivo del Control es contrastar el resultado final obtenido contra el deseado a fin de incorporar las correcciones necesarias para alcanzarlo, o bien verificar la efectividad de lo obtenido.

9.3.3 PLAN DE CONTINGENCIA

Pese a todas las medidas de seguridad puede (va a) ocurrir un desastre. De hecho los expertos en seguridad afirman "sutilmente" que hay que definir un plan de recuperación de desastres "para cuando falle el sistema", no "por si falla el sistema"[14].

Por tanto, es necesario que el Plan de Contingencias que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

Un **Plan de Contingencia de Seguridad Informática** consiste los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas.

---

[12] "Encuesta de Seguridad Informática 2001". Marzo de 2001. Ernst & Young. *http://www.ey.com*

[13] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. *http://www.cybsec.com*

[14] POYATO, Chelo. COLL, Francisco. MORENO, David. Recomendaciones de Seguridad. Definición de una Política de Seguridad. *http://www.rediris.es/cert*

Se entiende por **Recuperación**, "tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información"[15].

Se dice que el Plan de Contingencias es el encargado de sostener el modelo de Seguridad Informática planteado y de levantarlo cuando se vea afectado.

La recuperación de la información se basa en el uso de una política de copias de seguridad (Backup) adecuada.

9.3.4 EQUIPOS DE RESPUESTA A INCIDENTES

Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos proactivos del profesional de la seguridad. Entre éstos se incluyen:

- El desarrollo de instrucciones para controlar incidentes.
- Creación del sector o determinación del responsable: usualmente la designación del Administrador de seguridad.
- La identificación de las herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas de Seguridad Informática.
- La realización de actividades formativas y de motivación.
- La realización de investigaciones acerca de virus.
- La ejecución de estudios relativos a ataques al sistema.

Estos trabajos proporcionarán los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes.

Una vez que el Administrador de seguridad y el equipo de respuesta a incidentes han realizado estas funciones proactivas, el Administrador debe delegar la responsabilidad del control de incidentes al equipo de respuesta. Esto no significa que el Administrador no deba seguir implicado o formar parte del equipo, sino que no tenga que estar siempre disponible, necesariamente, y que el equipo debe ser capaz de controlar los incidentes por sí mismo.

El equipo será el responsable de responder a incidentes como virus, gusanos o cualquier otro código dañino, invasión, engaños, y ataques del personal interno. El equipo también debe participar en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos o de la red.

[15] POYATO, Chelo. COLL, Francisco. MORENO, David. Recomendaciones de Seguridad. Definición de una Política de Seguridad. *http://www.rediris.es/cert*

9.3.5 BACKUPS

El Backup de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backup, simplemente, es imposible volver la información al estado anterior al desastre.

Como siempre, será necesario realizar un análisis Costo/Beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el backup, etc.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

1. Se debe de contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.
2. Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.
3. El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.
4. Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.
5. Se debe de contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
6. Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se debe encriptar antes de respaldarse.
7. Se debe de contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
8. Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:

    - **Modalidad Externa:** otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.
    - **Modalidad Interna:** se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

Se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios. Por ejemplo, existe información que es función de otra (checksums). Si sólo se almacenara la información principal, sin sus checksums, esto puede derivar en la inutilización de la misma cuando se recupere el backup.

9.3.6 PRUEBAS

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados (Ethical Hacking) en sistemas de pruebas o en laboratorios permiten evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia.

Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede imposibilitar la realización de ataques simulados. Para asegurar los fondos necesarios para las pruebas, es importante que los directivos sean conscientes de los riesgos y consecuencias de los ataques, así como de las medidas de seguridad que se pueden adoptar para proteger al sistema, incluidos los procedimientos de las pruebas. Si es posible, se deben probar físicamente y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad posibles que se van a implementar.

Determinados ataques, por ejemplo desastres naturales como inundaciones y rayos, no se pueden probar, aunque una simulación servirá de gran ayuda. Por ejemplo, se puede simular un incendio en la sala de servidores en el que todos los servidores hayan resultado dañados y hayan quedado inutilizables. Este caso puede ser útil para probar la respuesta de los Administradores y del personal de seguridad, y para determinar el tiempo que se tardará en volver a poner la organización en funcionamiento.

La realización de pruebas y de ajustes en las directivas y controles de seguridad en función de los resultados de las pruebas es un proceso iterativo de aprendizaje. Nunca termina, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

9.4 LA POLÍTICA

Después de nueve capítulos de detalles técnicos, legales, administrativos y humanos ha llegado la hora esperada por mí y espero por el lector. Las páginas que siguen tienen la intención de ofrecer un acercamiento a una metodología sistemática en la importante tarea de administrar la Seguridad Informática.

Como ya se ha mencionado, los fundamentos aquí expuestos NO deben ser tomados puntualmente en cada organización tratada. Deberán ser adaptados a la necesidad, requisitos y limitaciones de cada organización (o usuario individual) y, posteriormente requerirá actualizaciones periódicas asegurando el dinamismo sistemático ya mencionado.

9.4.1 NIVEL FÍSICO

El primer factor considerado, y el más evidente debe ser asegurar el sustrato físico del objeto a proteger. Es preciso establecer un perímetro de seguridad a proteger, y esta protección debe adecuarse a la importancia de lo protegido.

La defensa contra agentes nocivos conlleva tanto medidas proactivas (limitar el acceso) como normativas de contingencia (que hacer en caso de incendio) o medidas de recuperación (realizar copias de seguridad). El grado de seguridad solicitado establecerá las necesidades: desde el evitar el café y el tabaco en las proximidades de equipos electrónicos, hasta el establecimiento de controles de acceso a la sala de equipos.

Lo más importante es recordar que quien tiene acceso físico a un equipo tiene control absoluto del mismo. Por ello sólo deberían accederlo aquellas personas que sea estrictamente necesario.

9.4.1.1 AMENAZA NO INTENCIONADA (DESASTRE NATURAL)

El siguiente ejemplo ilustra una posible situación:

Una organización no cuenta con sistemas de detección y protección de incendios en la sala de servidores. El Administrador del sistema deja unos papeles sobre el aire acondicionado de la sala. Durante la noche el acondicionador se calienta y se inicia un incendio que arrasa con la sala de servidores y un par de despachos contiguos.

Directivas:

1. **Predecir Ataque/Riesgo:** Incendio
2. **Amenaza:** Desastre natural. Incendio
3. **Ataque:** No existe.
4. **Estrategia Proactiva:**
   a. Predecir posibles daños: pérdida de equipos e información.
   b. Determinar y minimizar vulnerabilidades: protección contra incendios.
   c. Evaluar planes de contingencia: backup de la información.
5. **Estrategia Reactiva:**
   a. Evaluar daños: perdida de hardware e información.
   b. Determinar su origen y repararlos: bloqueo del aire acondicionado.
   c. Documentar y aprender
   d. Implementar plan de contingencia: recuperar backups.
6. **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

9.4.2 NIVEL HUMANO

9.4.2.1 EL USUARIO

Estas son algunos de las consideraciones que se deberían tener en cuenta para la protección de la información:

1. Quizás el usuario contempla todas las noticias de seguridad con escepticismo, piensan que los Administradores son paranoicos y se aprovechan de las contadas situaciones dadas. Quizás tengan razón, pero se debe recordar que el mundo virtual no es más que una pequeña muestra del mundo físico, con el agregado que es el campo ideal de impunidad y anonimicidad.

2. Generalmente se considera que la propia máquina es poco importante para que un atacante la tenga en cuenta. Se debería recordar que este atacante no sabe quien está del otro lado del monitor, por lo que cualquier objetivo (en principio) es tan importante (o no) como cualquier otro.

   Ejemplo: Se instaló un Firewall personal en dos usuarios normales de Internet, utilizando modems y Windows 98 como sistema operativo. Los resultados obtenidos en los archivos de Logs de estos usuarios fueron los siguientes:

   Usuario 1 ubicado en Paraná (Entre Ríos–Argentina): 49 scaneos de puertos y 14 intentos de instalación de troyanos en 10 días.

   Usuario 2 ubicado en Buenos Aires (Argentina): 28 scaneos de puertos en 8 días.

   La pregunta ya no es ¿seré atacado?; a cambiando a ¿cuándo seré atacado?.

3. Generalmente se sobrevalora la capacidad de un atacante. Al contrario de la creencia popular no se necesita ser un Gurú para ingresar en una computadora y generalmente quienes lo hace son Script–Kiddies en busca de "diversión". De hecho un Gurú siempre tendrá "mejores cosas que hacer".

4. Convencerse de que TODOS los programas existentes tienen vulnerabilidades conocidas y desconocidas es muy bueno. Esta idea permite no sobrevalorar la seguridad de su sistema.

   Ejemplo: Un usuario dice a otro: "Yo utilizo Linux porque es más seguro que Windows". Esto es una falacia disfrazada: el usuario debería decir que Linux PUEDE ser más seguro que Windows. De hecho cualquier sistema bien configurado puede ser más seguro que uno que no lo está.

5. La Regla de Oro que todo usuario debe tomar como obligación (y su responsabilidad) es tomar la seguridad de su computadora en serio. Recordar que el eslabón más débil de una cadena equivale a la resistencia de la misma es muy bueno en este momento.

Ningún usuario inocente estará contento si su nombre aparece en la lista de posibles intruso en una red, nada más que porque alguien decidió utilizarlo para tales fines. Tampoco es bueno ser acusado de expandir un virus por el simple hecho de enviar mails sin comprobarlos anteriormente.

Los procedimientos simples mencionados pueden evitar grandes dolores de cabezas.

9.4.2.1.1 Amenaza no Intencionada (Empleado)

El siguiente ejemplo ilustra una posible situación de contingencia y el procedimiento a tener en cuenta:

Un empleado, no desea perder la información que ha guardado en su disco rígido, así que la copia (el disco completo) a su carpeta particular del servidor, que resulta ser también el servidor principal de aplicaciones de la organización. No se han definido cuotas de disco para las carpetas particulares de los usuarios que hay en el servidor. El disco rígido del usuario tiene 6 GB de información y el servidor tiene 6,5 GB de espacio libre. El servidor de aplicaciones deja de responder a las actualizaciones y peticiones porque se ha quedado sin espacio en el disco. El resultado es que se deniega a los usuarios los servicios del servidor de aplicaciones y la productividad se interrumpe.

A continuación, se explica la metodología que se debería haber adoptado antes de que el usuario decida realizar su copia de seguridad:

Directivas:

1. **Predecir Ataque/Riesgo:** Negación de servicios por abuso de recursos.
2. **Amenaza:** No existe. Empleado sin malas intenciones.
3. **Ataque:** No existe motivo ni herramienta, solo el desconocimiento por parte del usuario.
4. **Estrategia Proactiva:**
   a. Predecir posibles daños: pérdida de productividad por espacio de disco/memoria agotados.
   b. Determinar y minimizar vulnerabilidades: implementar cuotas de discos.
   c. Evaluar planes de contingencia: servidor backup.
   d. Capacitar el usuario.
5. **Estrategia Reactiva:**
   a. Evaluar daños: pérdida de producción.
   b. Determinar su origen y repararlos: hacer espacio en el disco.
   c. Documentar y aprender: implementar plan de contingencia.
6. **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

9.4.2.1.2 Amenaza Malintencionada (Insider)

Una empresa competidora ofrece a un usuario cierta suma de dinero para obtener el diseño del último producto desarrollado por su empresa. Como este usuario carece de los permisos necesarios para obtener el diseño se hace pasar como un Administrador, y usando ingeniería social, consigue el nombre de usuario y password de un usuario con los permisos que él necesita.

La política de seguridad asociada a este evento debería haber contemplado:

Directivas:

1. **Predecir Ataque/Riesgo:** Robo de información mediante el uso de ingeniería social.
2. **Amenaza:** Insider.
3. **Ataque:** Ingeniería social.
4. **Estrategia Proactiva:**
   a. Predecir posibles daños: pérdida de productividad y/o beneficios.
   b. Determinar y minimizar vulnerabilidades: concientización de los usuarios.
   c. Evaluar planes de contingencia.
5. **Estrategia Reactiva:**
   a. Evaluar daños: pérdida de beneficios e información.
   b. Determinar su origen: revelación de login y password por parte el usuario.
   c. Reparación de daños: implementar entrenamiento de los usuarios.
   d. Documentar y aprender.
   e. Implementar plan de contingencia.
6. **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

9.4.1.2 Personas Ajenas al Sistema

9.4.1.2.1 Amenaza No Intencionada

Un virus ingresa a la empresa mediante un mail enviado a un empleado, y comienza a expandirse dentro de la misma tomando como base la libreta de direcciones de los usuarios:

Directivas:

1. **Predecir Ataque/Riesgo:** Negación de servicio del servidor de correo electrónico por gran la cantidad de mensajes enviados/recibidos.
2. **Amenaza:** Virus.
3. **Ataque:** Virus de correo electrónico.
4. **Estrategia Proactiva:**
   a. Predecir posibles daños: pérdida de productividad por negación de servicio.
   b. Determinar y minimizar vulnerabilidades: actualización de antivirus y concientización de usuarios en el manejo del correo electrónico.
   c. Evaluar planes de contingencia: evaluar la importancia de un servidor backup. Antivirus.
5. **Estrategia Reactiva:**
   a. Evaluar daños: pérdida de producción.
   b. Determinar su origen: caída del servidor por overflow de mensajes.
   c. Reparación de daños: implementar el servidor backup. Eliminación del virus causante del problema.
   d. Documentar y aprender.
   e. Implementar plan de contingencia: servidor backup.
6. **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

9.4.1.2.2 Amenaza Malintencionada (Out–Sider)

Una persona ingresa al sistema de la empresa, con intenciones de recopilar información para su posterior venta:

Directivas:

7. **Predecir Ataque/Riesgo:** Ingreso al sistema por vulnerabilidades en los sistemas o política de claves ineficiente.
8. **Amenaza:** Outsider recopilando información significativa.
9. **Ataque:** Ingreso al sistema.
10. **Estrategia Proactiva:**
    a. Predecir posibles daños: Robo y venta de información. Daño a la imágen de la empresa.
    b. Determinar y minimizar vulnerabilidades: actualización de sistemas vulnerables. Concientización a los usuarios en el manejo de contraseñas fuertes.
    c. Evaluar planes de contingencia: implementación de servidor backup para casos de daño de la información. Recuperación de imagen. Evaluar formas de minimizar el daño por la información robada.
11. **Estrategia Reactiva:**
    f. Evaluar daños: información susceptible robada.
    g. Determinar su origen: ingreso al sistema.
    h. Reparación de daños.
    i. Documentar y aprender.
    j. Implementar plan de contingencia: servidor backup.
12. **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.