RESOLUCIÓN 129

POR CUANTO: El Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional" de 5 de junio de 2019 establece en su Artículo 19 que el diseño del Sistema de Seguridad Informática y la elaboración del Plan de Seguridad Informática de cada entidad se realizan en correspondencia con las metodologías establecidas por el Ministerio de Comunicaciones, por lo que se considera necesario establecer la Metodología para la Gestión de la Seguridad Informática en todo el país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar la Metodología para la Gestión de la Seguridad Informática que se anexa y que forma parte integrante de la presente Resolución.

SEGUNDO: Las entidades disponen de ciento ochenta días contados a partir de la entrada en vigor de la presente Resolución, para establecer sus Sistemas de Gestión de la Seguridad Informática, en correspondencia con lo regulado en la referida metodología.

TERCERO: La Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones es la encargada de ejercer el control del cumplimiento de lo dispuesto en la presente Resolución.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas, la Metodología para la Gestión de la Seguridad Informática.

NOTIFÍQUESE al director general de la Oficina de Seguridad para las Redes Informáticas.

COMUNÍQUESE a los viceministros, al director general de Informática y al director de Regulaciones del Ministerio de Comunicaciones.

Ave. Independencia No.2 e/ 19 de Mayo y Aranguren, La Habana, Cuba. Telef. (+537) 859-9205 / (+537) 859-9206
Fax: (537) 859-9232 Correo electrónico: despacho@mincom.gob.cu

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los días 24 del mes de junio del 2019.

Jorge Luis Perdomo Di-Lella

REPÚBLICA DE CUBA
MINISTRO DE COMUNICACIONES

ANEXO

METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA

ÍNDICE

Segunda Parte: Estructura y contenido del Plan de Seguridad Informática

1. Alcance del Plan de Seguridad Informática
2. Caracterización del Sistema Informático
3. Resultados del Análisis de Riesgos
4. Políticas de Seguridad Informática
5. Responsabilidades
6. Medidas y Procedimientos de Seguridad Informática
   - 6.1. Clasificación y control de los bienes informáticos
   - 6.2. Del Personal
   - 6.3. Seguridad Física y Ambiental
   - 6.4. Seguridad de Operaciones
   - 6.5. Identificación, Autenticación y Control de Acceso
   - 6.6. Seguridad ante programas malignos
   - 6.7. Respaldo de la Información
   - 6.8. Seguridad en Redes
   - 6.9. Gestión de Incidentes de Seguridad
7. Anexos del Plan de Seguridad Informática
   - 7.1 Listado nominal de Usuarios con acceso a los servicios de red
   - 7.2 Registros
   - 7.3 Control de Cambios

Objeto

La presente metodología tiene por objeto determinar las acciones a realizar en una entidad durante el diseño, la implementación y posterior operación de un Sistema de Gestión de la Seguridad Informática, en lo adelante SGSI, compuesta por dos partes, la primera se dedica al SGSI y la segunda a la estructura y contenido del Plan de Seguridad Informática.

Constituye un complemento a lo exigido en el Decreto de Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional y el Reglamento de Seguridad para las Tecnologías de la Información y la Comunicación en cuanto a la obligación de diseñar, implantar y mantener actualizado un Sistema de Seguridad Informática, a partir de los bienes a proteger y de los riesgos a que están sometidos.

Alcance

Esta metodología está dirigida a todas las personas vinculadas con las Tecnologías de la Información y la Comunicación, en lo adelante TIC, de una entidad, ya sea por la responsabilidad que tienen asignadas en relación con los bienes informáticos o por los beneficios que de ellos obtienen.

Los primeros destinatarios de esta metodología son los directivos y funcionarios de los distintos niveles de una entidad, que responden por el buen funcionamiento de las tecnologías y la información que en ellas se procesa.

Términos y definiciones

A los efectos de la presente metodología se entiende por:

1. **Análisis de riesgos:** proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos, e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.
2. **Identificación de usuarios:** identificador (ID) que define quién es el usuario y qué lo identifica unívocamente en el sistema, diferenciándolo en los sistemas multiusuario del resto.
3. **Impacto:** daño producido por la materialización de una amenaza.
4. **Riesgo residual:** riesgo remanente después de aplicados controles de seguridad para minimizarlo.

5. **Sistema informático:** conjunto de bienes informáticos de que dispone una entidad para su correcto funcionamiento y la consecución de sus objetivos.
6. **Soportes removibles:** cualquier tipo de dispositivo intercambiable que permita la transferencia o almacenamiento de información.
7. **Trazas de auditoría:** registros que se generan para describir la información asociada a eventos de interés en los diferentes procesos que se ejecutan en las TIC; están compuestos por secciones y campos donde se describen aspectos como fecha y hora, tipo de evento, quién o qué lo causa, y qué se afecta, que permiten comprender el evento que se registra y usualmente se registran en orden cronológico.

El SGSI de una entidad se diseña con la consideración del conjunto de sus bienes informáticos a partir de su importancia y el papel que representan para el cumplimiento de su actividad, por lo que se presta especial atención a aquellos que son críticos en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo a que están sometidos.

Un SGSI conlleva la conformación de una estrategia sobre cómo tratar los aspectos de seguridad e implica la implementación de los controles necesarios para garantizar el cumplimiento de lo establecido en esta materia, a partir de un análisis de riesgos que incluya:

1. determinar qué se trata de proteger;
2. determinar de qué es necesario protegerse;
3. determinar cuan probables son las amenazas;
4. implementar los controles que protejan los bienes informáticos de una manera rentable; y
5. revisar continuamente este proceso y perfeccionarlo cada vez que una debilidad (vulnerabilidad) sea encontrada.

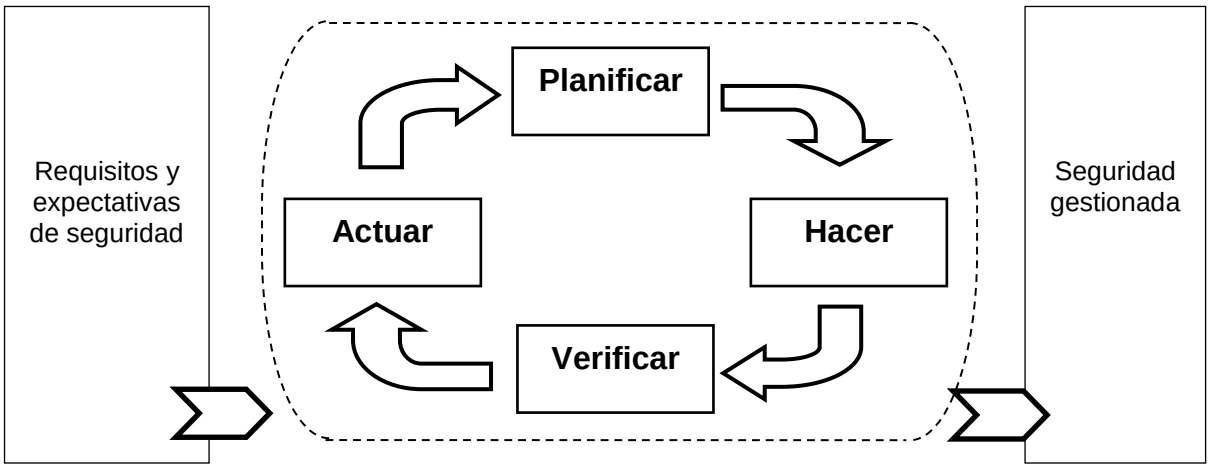
Los tres primeros aspectos son imprescindibles para tomar decisiones efectivas sobre seguridad. Sin un conocimiento razonable de lo que se quiere proteger, contra qué protegerlo y cuan probables son las amenazas, seguir adelante carece de sentido.
La presente metodología promueve la adopción de un enfoque basado en procesos, con el fin de establecer, implementar, operar, dar seguimiento, mantener y mejorar el SGSI de una organización; para ello adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), que se aplica para estructurar todos los procesos del SGSI en correspondencia con la NC-ISO-IEC 27001“Requisitos de los Sistema de Gestión de la

Seguridad de la Información" y adecuada a la NC-ISO-IEC 17799 (27002) "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".

Primera Parte: Sistema de Gestión de la Seguridad Informática

Procesos de un Sistema de Gestión de la Seguridad Informática

El SGSI se compone de cuatro procesos básicos:



Modelo PHVA aplicado a los procesos del SGSI

Planificar (Establecer el SGSI)	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de entregar resultados acordes con las políticas y objetivos globales de la organización.
Hacer (Implementar y operar el SGSI)	Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y su correcta aplicación.
Verificar (Revisar y dar seguimiento al SGSI)	Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (Mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI.

1. Proceso de Planificación del SGSI

Objetivo principal: La realización del análisis y evaluación de los riesgos de seguridad y la selección de controles adecuados.

En esta primera etapa se crean las condiciones para la realización del diseño, implementación y gestión del Sistema de Seguridad Informática, para lo cual se realiza un estudio de la situación del sistema informático desde el punto de vista de la seguridad, con el fin de determinar las acciones que se ejecutan en función de las necesidades detectadas y con ello establecer las políticas, los objetivos, procesos y procedimientos de seguridad apropiados para gestionar el riesgo y mejorar la seguridad informática, lo cual posibilita obtener resultados conformes con las políticas y objetivos globales de la organización.

Los bienes informáticos de que dispone una entidad no tienen el mismo valor, e igualmente, no están sometidos a los mismos riesgos, por lo que es imprescindible la realización de un análisis de riesgos que ofrezca una valoración de los bienes informáticos y las amenazas a las que están expuestos, así como una definición de la manera en que se gestionan dichos riesgos para reducirlos.

Como resultado, se establecen las prioridades en las tareas a realizar para minimizar los riesgos, puesto que estos nunca desaparecen totalmente. La dirección de la entidad asume el riesgo residual, o sea, el nivel restante de riesgo después de su tratamiento.

1.1 Preparación

Durante la preparación se crean las condiciones para el diseño e implementación del SGSI, y se consideran los aspectos siguientes:

1. Asegurar el compromiso de la dirección.
2. Seleccionar y preparar a los miembros del equipo que participa en el diseño e implementación del SGSI.
3. Recopilar información de seguridad.

1.1.1. Compromiso de la dirección de la entidad con la Seguridad Informática

La dirección apoya activamente la seguridad dentro de la organización mediante una orientación clara, compromiso demostrado y la asignación explícita de las responsabilidades de seguridad informática y su reconocimiento, para lo cual:

a) Asegura que los objetivos de seguridad informática estén identificados, cumplan los requisitos de la organización y están integrados en los procesos principales;
b) formula, revisa y aprueba las políticas de seguridad informática;
c) revisa la efectividad de la implementación de las políticas de seguridad;
d) provee una orientación clara y apoyo visible hacia las iniciativas de seguridad;
e) proporciona los recursos necesarios para la seguridad;
f) aprueba la asignación de los roles específicos y responsabilidades en seguridad informática en la organización;
g) inicia planes y programas para mantener la concienciación en seguridad; y
h) asegura que la implementación de los controles de seguridad informática sea coordinada en toda la organización.

1.1.2. Seleccionar y preparar a los miembros del equipo que participan en el diseño e implementación del SGSI

El proceso de diseño e implementación del SGSI no se realiza por una sola persona o por un grupo de personas de una misma especialidad, sino que es el resultado de un trabajo multidisciplinario en el que participen todos aquellos que de manera integral puedan garantizar el cumplimiento de los objetivos planteados.

El equipo de diseño e implementación se conforma con:

1. Directivos y funcionarios que, a los diferentes niveles, responden por la información que se procesa en las tecnologías y por tanto son los garantes de su protección.
2. Personal de informática que domina los aspectos técnicos necesarios para la implementación de los controles de seguridad.
3. Profesionales de la protección, a partir de su responsabilidad en la custodia de los bienes informáticos y otros que se consideren de acuerdo con su perfil.

1.1.3. Recopilar información de seguridad

Durante el proceso de preparación se reúne toda la información que facilite el diseño e implementación del SGSI, para lo que se utilizan los documentos normativos y

metodológicos que existan sobre el tema; documentación de aplicaciones y sistemas en explotación en la organización; documentación de incidentes ocurridos en la entidad o en otras organizaciones afines; tendencias de seguridad nacionales e internacionales, así como otros materiales que faciliten su realización.

1.2. Determinación de las necesidades de protección

Las necesidades de protección del sistema informático se establecen mediante la realización de un análisis de riesgos, que es el proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.

La realización del análisis de riesgos proporciona:

a) Una detallada caracterización del sistema informático objeto de protección;
b) la creación de un inventario de bienes informáticos a proteger;
c) la evaluación de los bienes informáticos a proteger en orden de su importancia para la organización;
d) la identificación y evaluación de amenazas y vulnerabilidades;
e) la estimación de la relación importancia-riesgo asociada a cada bien informático (peso de riesgo).

En el proceso de análisis de riesgos se pueden diferenciar dos aspectos:

1. La **Evaluación de Riesgos** orientada a determinar los sistemas que, en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, valoran los riesgos y establecen sus niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la entidad; consiste en el proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar su importancia.
2. La **Gestión de Riesgos** que implica la identificación, selección, aprobación y manejo de los controles a establecer para eliminar o reducir los riesgos evaluados a niveles aceptables, con acciones destinadas a:
   a) Reducir la probabilidad de que una amenaza ocurra;
   b) limitar el impacto de una amenaza, si esta se manifiesta;
   c) reducir o eliminar una vulnerabilidad existente; y
   d) permitir la recuperación del impacto o su transferencia a terceros.

La gestión de riesgos implica la clasificación de las alternativas para manejar los riesgos a que puede estar sometido un bien informático dentro de los procesos en una entidad; implica una estructura bien definida, con controles adecuados y su conducción mediante acciones factibles y efectivas. Para ello se cuenta con las técnicas de manejo del riesgo siguientes:

1. **Evitar:** impedir el riesgo con cambios significativos en los procesos por mejoramiento, rediseño o eliminación, y es el resultado de adecuados controles y acciones realizadas.
2. **Reducir:** cuando el riesgo no puede evitarse por dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible; esta opción es la más económica y sencilla y se consigue con la optimización de los procedimientos y con la implementación de controles.
3. **Retener:** cuando se reduce el impacto de los riesgos pueden aparecer riesgos residuales; dentro de las estrategias de gestión de riesgos de la entidad se plantea como manejarlos para mantenerlos en un nivel mínimo.
4. **Transferir:** es buscar un respaldo contractual para compartir el riesgo con otras entidades, por ejemplo alojamiento, hospedaje, externalización de servicios, entre otros; esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar este.

La necesidad de la actualización permanente del análisis de riesgos está determinada por las circunstancias siguientes:

a) Los elementos que componen un sistema informático en una entidad están sometidos a constantes variaciones: cambios de personal, nuevos locales, nuevas tecnologías, nuevas aplicaciones, reestructuración de entidades, nuevos servicios y otros;
b) la aparición de nuevas amenazas o la variación de la probabilidad de ocurrencia de alguna de las existentes; y
c) pueden aparecer nuevas vulnerabilidades o variar o incluso desaparecer alguna de las existentes, y originan, modifican o eliminan posibles amenazas.

En resumen, durante la determinación de las necesidades de protección del sistema informático es necesario:

1. Caracterizar el sistema informático.
2. Identificar las amenazas potenciales y estimar los riesgos sobre los bienes informáticos.

3. Evaluar el estado actual de la seguridad.

1.2.1 Caracterización del sistema informático

Para el diseño e implementación de cualquier sistema es imprescindible el conocimiento pleno del objeto sobre el cual se quiere diseñar o implantar. Para ello lo más apropiado es precisar los elementos que permitan identificar sus especificidades.

La caracterización del sistema informático incluye la determinación de los bienes informáticos que requieren ser protegidos, su valoración y clasificación según su importancia.

Se precisan los datos que permitan determinar cómo fluye la información entre los diferentes elementos de la entidad, así como entre la entidad y otras instituciones; se considera el carácter de la información y su nivel de clasificación de acuerdo con lo establecido en el país.

Durante la caracterización del sistema informático es necesario establecer además las características de las edificaciones y locales donde están instalados los equipos, tipo de construcción y estructura, lugares o puntos de acceso (ventanas y puertas), visibilidad desde el exterior, ubicación de las TIC, tipos de tecnologías, software instalado, nivel de clasificación de la información que se procesa, documentación de software, preparación y conocimiento del personal que opera los equipos, cualquier otro aspecto que haga más precisa su descripción.

Una buena caracterización del sistema informático permite conocerlo a plenitud y evita pérdida de tiempo e imprecisiones.

Una posible agrupación por categorías que puede ayudar a la identificación de los bienes informáticos a proteger, podría ser la siguiente:

1. **Hardware:** redes de diferente tipo, servidores y estaciones de trabajo, computadoras personales (incluyen portátiles), soportes magnéticos, ópticos y removibles, líneas de comunicaciones, módems, ruteadores, concentradores, entre otros.
2. **Software:** programas fuentes, programas ejecutables, programas de diagnóstico, programas utilitarios, sistemas operativos, programas de comunicaciones, entre otros.

3. **Datos:** generados durante la ejecución, almacenados en discos, información de respaldo, bases de datos, trazas de auditoría, en tránsito por los medios de comunicaciones, entre otros.
4. **Personas:** usuarios, operadores, programadores, personal de mantenimiento, entre otros.
5. **Documentación:** de programas, de sistemas, de hardware, de procedimientos de administración, entre otros.

Una vez identificados los bienes informáticos que necesitan ser protegidos, se determina su importancia dentro del sistema informático y se clasifican según esta.

La valoración de los bienes informáticos posibilita mediante su categorización, determinar en qué medida uno es más importante que otro (grado de importancia) y se toman en cuenta aspectos tales como: la función que realizan, su costo, la repercusión que ocasionaría la pérdida y posibilidad de su recuperación; así como la preservación de la confidencialidad, la integridad y la disponibilidad.

Al estimar la repercusión que ocasiona la pérdida de un bien informático se tiene en cuenta el tiempo que la entidad puede seguir el trabajo sin este, lo que puede ser vital para su funcionamiento. Este tiempo puede oscilar entre escasas horas, hasta días y semanas. Por ejemplo: una agencia bancaria no puede prescindir de su Plan de Cuentas por un número considerable de horas, porque sería imposible su funcionamiento.

Se da el caso que un bien informático puede estar hasta tres semanas dañado. Esto depende de su ciclo de utilización, por ejemplo: si la nómina de una entidad se daña días antes del pago a los trabajadores pondría a la entidad en un serio aprieto, si se dañó después del cobro, habría más tiempo para su recuperación.

La determinación de la importancia de cada bien informático puede ser realizada de forma descriptiva (por ejemplo, valor alto, medio, bajo) o de forma numérica asignan valores entre cero y diez (0 si tiene poca importancia y 10 sí es máxima).

Un resultado inmediato de la caracterización del sistema informático es la conformación de un listado que contenga la relación de los bienes informáticos identificados y clasificados según su importancia.

Bienes informáticos críticos

Como resultado de la evaluación anterior se determinan los bienes informáticos críticos para la gestión de la entidad en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo a que están sometidos. Se consideran bienes informáticos críticos aquellos sin los cuales el trabajo de la entidad no tuviera sentido o no puede ser ejecutado. Por ejemplo:

a) El servidor principal de una red;
b) los medios de comunicaciones de un centro de cobros y pagos remoto;
c) el sistema de control de tráfico aéreo de un aeropuerto;
d) el sistema contable de una entidad.

Los bienes informáticos críticos tienen carácter relativo según la entidad de que se trate, por ejemplo: la destrucción o modificación de una base de datos en una escuela secundaria probablemente no tenga la misma connotación que si ocurre en un centro de investigaciones científicas.

Un aspecto de vital importancia es la concatenación, o sea, la dependencia entre un bien informático y otro. En la práctica se da el caso que un bien informático resulta no ser importante tratado individualmente, para el correcto funcionamiento de una tarea cualquiera, pero como elemento de un sistema, es el preámbulo o paso anterior obligado para el funcionamiento de otro bien informático que ha sido marcado como importante. En este caso todos los activos que cumplen con esa condición han de ser considerados como importantes.

Por otra parte, puede que un recurso sea muy costoso y por ello considerado de importancia alta, y sin embargo no es imprescindible para la gestión de la entidad. Estas circunstancias pueden elevar de forma artificial el nivel de importancia con que ha sido catalogado.

El equipo de trabajo controla que las distintas estructuras que conforman la entidad no declaren importantes aquellos bienes informáticos que en realidad no lo son. Esto evitaría gastos innecesarios. Existe la tendencia de declarar como importantes (críticos) a bienes informáticos que en realidad no lo son. A la hora de tratar este aspecto el equipo de trabajo es lo suficientemente paciente y persuasivo para evitar esta perjudicial práctica.

Lo anterior implica un análisis complementario de los datos obtenidos en el listado de bienes informáticos, que se realiza de la forma siguiente:

1. Señale adecuadamente aquellos bienes informáticos que fueron valorados de importancia significativa.
2. Señale aquellos bienes informáticos, que no han sido valorados de importancia significativa, y tienen una incidencia directa con algún otro bien informático crítico.
3. Señale después de un estudio riguroso y detallado, aquellos bienes informáticos que no tienen una valoración significativa, ni incidencia directa en el trabajo de bienes informáticos críticos, y resulta necesario que sean marcados como tales, por razones prácticas.
4. Ordene el listado de bienes informáticos a partir de las consideraciones anteriores.

1.2.2. Identificación de las amenazas sobre el sistema informático

Una vez que los bienes informáticos que requieren protección son identificados y valorados según su importancia, es necesario identificar las amenazas sobre éstos y estimar el daño (impacto) que puede producir su materialización.

Para cada bien informático a proteger los objetivos fundamentales de seguridad son la confidencialidad, la integridad y la disponibilidad, por lo que hay que determinar cada amenaza sobre la base de como pueda afectar a estas características de la información. El peso que cada una de estas características tiene para los bienes informáticos varía de una entidad a otra, en dependencia de la naturaleza de los procesos informáticos que se llevan a cabo en función de su objeto social. Algunas de las amenazas más comunes son las siguientes:

a) pérdida de información;
b) corrupción o modificación de información;
c) sustracción, alteración o pérdida de equipos o componentes;
d) divulgación de información; e
e) interrupción de servicios.

La realización de un análisis de riesgos implica el examen de cada una de las amenazas sobre los bienes informáticos y su clasificación por niveles, a partir de la probabilidad de su ocurrencia y la severidad del impacto que puedan producir.

1.2.3. Estimación del riesgo sobre los bienes informáticos

La estimación del riesgo sobre cada bien informático se determina con la consideración de las probabilidades de materialización de las amenazas que actúan sobre este. Esto puede ser realizado de forma descriptiva (por ejemplo: riesgo alto, medio, bajo) o de forma numérica asignan valores entre cero y uno (0 sí la probabilidad de que se materialice la amenaza es nula y 1 si es máxima).

Una amenaza puede incidir sobre varios bienes informáticos con la misma probabilidad y sin embargo sus consecuencias no necesariamente son iguales, dependen en cada caso de la importancia del bien de que se trate. La interrelación entre la probabilidad de materialización de las amenazas que actúan sobre un bien informático y la importancia estimada de este, determinan el peso del riesgo. De esta manera se puede determinar el peso del riesgo para cada bien informático.

La evaluación de los riesgos posibilita conocer que bienes informáticos, o que áreas en particular están sometidas a un mayor peso de riesgo y su naturaleza, lo que permite la selección adecuada de los controles de seguridad que son establecidos en cada uno de los casos, y se garantiza de esta manera una correcta proporcionalidad por medio de una adecuada relación entre costos y beneficios.

Es necesario precisar de una manera exhaustiva los riesgos a que está sometido el sistema en cada una de sus partes componentes, a partir de lo cual se pueden determinar con racionalidad los controles de seguridad que son implementados.

La aplicación de los elementos aquí expuestos puede ser realizada con mayor o menor rigor, en dependencia de la composición y preparación del equipo de trabajo designado para acometer esta tarea y de la participación que se dé a otras personas, que sin formar parte del equipo, puedan brindar los elementos que se requiera.

Por otra parte, desde el momento que los resultados dependen de valores estimados, las conclusiones a que se arribe son tomadas como una aproximación al problema, que puede ser ajustada en sucesivas versiones, en correspondencia con la práctica diaria. Los conceptos anteriormente expresados pueden ser aplicados en diversas variantes, pero de alguna forma es imprescindible utilizarlos.

1.2.4. Evaluación del estado actual de la Seguridad Informática

Generalmente las entidades que emplean las TIC en el desarrollo de su actividad, aunque no hayan diseñado un sistema de seguridad informática que considere de forma integral todos los factores a tener en cuenta, tienen implementadas determinadas normas, medidas y procedimientos de seguridad, generalmente de forma empírica a partir de incidentes que han ocurrido o de las experiencias de otras entidades, lo que es insuficiente y da lugar a la existencia de vulnerabilidades.

Es necesario evaluar de manera crítica la efectividad de los controles existentes, sobre la base de los resultados del análisis de riesgos realizado, con el objetivo de perfeccionarlos o sustituirlos por aquellos que brinden la respuesta adecuada. Los resultados de esta evaluación ayudan a orientar y a determinar una apropiada acción gerencial y las prioridades para gestionar los riesgos de seguridad informática, así como la implementación de los controles seleccionados para protegerse.

La determinación de las necesidades de protección examinada en este apartado da como resultado la definición de los aspectos principales siguientes:

1. Cuáles son los bienes informáticos más importantes a proteger.
2. Que amenazas tienen mayor probabilidad de actuar sobre los bienes informáticos y su posible impacto sobre la entidad.
3. Que áreas están sometidos a un mayor peso de riesgo y que amenazas los motivan.
4. Que controles de seguridad son perfeccionados o sustituidos y en qué caso se requiere definir e implementar alguno nuevo.

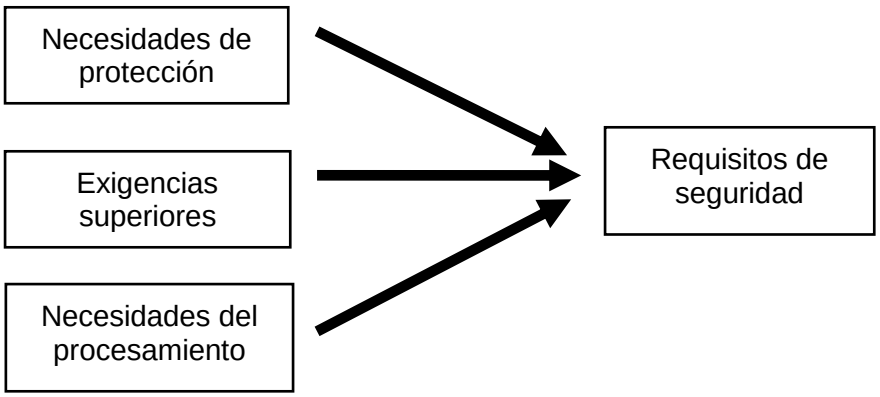
Llegado a este punto es necesario:

1. Identificar y evaluar alternativas posibles para tratar los riesgos.
2. Seleccionar e implantar los controles que permitan reducir el riesgo a un nivel aceptable.
3. Identificar los riesgos residuales que han quedado sin cubrir.
4. Preparar un plan para el tratamiento de los riesgos.
5. Preparar procedimientos para implantar los controles.

1.3 Establecimiento de los requisitos de Seguridad Informática

Parte esencial del proceso de planificación consiste en la identificación de los requisitos de seguridad de la organización. Existen tres fuentes principales:

1. La determinación de las necesidades de protección de la organización, durante la cual se identifican los bienes informáticos más importantes; las amenazas a que están sometidos; se evalúa la vulnerabilidad y la probabilidad de ocurrencia de las amenazas y se estima su posible impacto.
2. El conjunto de requisitos instituidos por obligaciones contractuales, normas legales y técnicas que satisfacen la organización.
3. Los principios, objetivos y requisitos que forman parte del procesamiento de la información que la organización ha desarrollado para apoyar sus operaciones.



Los requisitos de seguridad se identifican mediante la evaluación de los riesgos. El gasto en controles se equilibra con el perjuicio para la organización resultante de los fallos de seguridad (costo-beneficio).

1.4 Selección de los controles de Seguridad Informática

Antes de considerar el tratamiento de los riesgos, la organización decide los criterios para determinar si pueden ser aceptados o no. Un riesgo puede ser aceptado si, por ejemplo, se determina que es bajo o que el costo de su tratamiento no es rentable para la organización.

Para cada uno de los riesgos identificados se toma una decisión sobre su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

a) **Aplicar controles apropiados** para reducir los riesgos;
b) **Aceptar riesgos** de manera consciente y objetiva, siempre que satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos;
c) **Evitar riesgos**, no permitir las acciones que propicien los riesgos;
d) **Transferir los riesgos** a otras partes, por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde se decida aplicar controles apropiados, se seleccionan e implantan para lograr los requisitos identificados mediante la evaluación de riesgos. Los controles aseguran que estos son reducidos a un nivel aceptable y se toman en cuenta:

a) requisitos y restricciones de la legislación y de las regulaciones nacionales e internacionales;
b) objetivos de la organización;
c) requisitos y restricciones operacionales;
d) costo de la implementación y de la operación;
e) la necesidad de balancear la inversión en la implementación y la operación de controles contra el daño probable como resultado de fallas de la seguridad.

Los controles de seguridad que se seleccionen para la reducción de los riesgos a un nivel aceptable cubren adecuadamente las necesidades específicas de la organización. La selección de los controles de seguridad depende de una decisión organizacional basada en los criterios para la aceptación del riesgo, las opciones para su tratamiento, y el acercamiento a su gestión general aplicada a la organización, y también está conforme con toda la legislación y regulaciones nacionales e internacionales vigentes.

Los objetivos de control y los controles se basan en: los resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo; en los requisitos legales o reglamentarios; en las obligaciones contractuales y en las necesidades orgánicas de la entidad en materia de seguridad informática.

Los controles de seguridad informática son considerados en las etapas de especificación de requisitos y de diseño de sistemas y aplicaciones. El no hacerlo puede dar lugar a costos adicionales y a soluciones menos eficaces, y en el peor de los casos, imposibilidad de alcanzar la seguridad adecuada. Estos controles son establecidos, implementados,

supervisados y mejorados cuando sea necesario para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

Hay que tener presente que ningún sistema de controles puede alcanzar la seguridad completa y que acciones adicionales de gestión se implementan para supervisar, evaluar, y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la organización.

La seguridad informática se logra implantar con un conjunto adecuado de controles, que incluyen políticas, procesos, medidas, procedimientos, estructuras organizativas y funciones de hardware y software. Nos referiremos a continuación específicamente a las políticas y a las medidas y procedimientos de seguridad informática.

1.4.1. Políticas de Seguridad Informática

El objetivo fundamental de la definición de las Políticas de Seguridad Informática consiste en proporcionar orientación y apoyo de la dirección para la seguridad informática, de acuerdo con los requisitos de la organización y con las regulaciones y leyes vigentes.

La dirección establece políticas de seguridad en correspondencia con los objetivos de la entidad y demuestra su apoyo y compromiso a la seguridad informática, con la publicación y el mantenimiento de esas políticas en toda la organización, las cuales se comunican a todos los usuarios de manera apropiada, accesible y comprensible.

Las políticas de seguridad definen los “QUE”: **qué** debe ser protegido, **qué** es más importante, **qué** es más prioritario, **qué** está permitido y **qué** no lo está y **qué** tratamiento se le dan a los problemas de seguridad. Las políticas de seguridad en sí mismas no dicen “COMO” las cosas son protegidas. Esto es función de las medidas y procedimientos de seguridad.

Las políticas de seguridad conforman la estrategia general. Las medidas y procedimientos establecen en detalle los pasos requeridos para proteger el sistema informático. No puede haber medidas y procedimientos que no respondan a una política, al igual que no puede concebirse una política que no esté complementada con las medidas y procedimientos que le correspondan.

Comenzar con la definición de las políticas de seguridad a partir de los riesgos estimados asegura que las medidas y procedimientos proporcionen un adecuado nivel de protección para todos los bienes informáticos.

Desde que las políticas de seguridad pueden afectar a todo el personal en una entidad es conveniente asegurar tener el nivel de autoridad requerido para su establecimiento. La creación de las políticas de seguridad es avalada por la máxima dirección de la organización que tiene el poder de hacerlas cumplir. Una política que no se puede implementar y hacer cumplir es inútil.

Uno de los objetivos básicos al desarrollar las políticas de seguridad consiste en definir qué se considera uso apropiado de los sistemas informáticos; así como la forma en que se tratan los incidentes de seguridad. Para esto son considerados los criterios siguientes:

1. Tener en cuenta el objeto social de la entidad y sus características. Por ejemplo la seguridad de una entidad comercial es muy diferente a la de un organismo central o a la de una universidad.
2. Las políticas de seguridad que se desarrollen están en correspondencia con las políticas, reglas, regulaciones y leyes a las que la entidad está sujeta.
3. A menos que el sistema informático a proteger esté completamente aislado e independiente, hay que considerar las implicaciones de seguridad en un contexto más amplio. Las políticas manejan los asuntos derivados de un problema de seguridad que tiene lugar por causa de un sitio remoto, así como un problema que ocurre en este como resultado de un usuario o computadora local.

Algunas de las interrogantes que se resuelven al diseñar una política de seguridad son las siguientes:

1. ¿Qué estrategia se adopta para la gestión de la seguridad informática?
2. ¿A quién se le permite utilizar los bienes informáticos?
3. ¿Qué se entiende por uso correcto de los recursos?
4. ¿Quién está autorizado para garantizar el acceso y aprobar el uso de los bienes informáticos?
5. ¿Quién tiene privilegios de administración de los sistemas?
6. ¿Cuáles son los derechos y responsabilidades de los usuarios?
7. ¿Cuáles son los derechos y responsabilidades de los administradores de sistemas frente a los de los usuarios?
8. ¿Qué hacer con la información clasificada y limitada?

9. ¿Qué hacer ante la ocurrencia de un incidente de seguridad?

Estas no son las únicas interrogantes que son resueltas en el diseño de las políticas. En la práctica surgen otras no menos importantes.

Las principales características que tiene una buena política de seguridad son:

1. Poder implementarse a través de medidas y procedimientos, la publicación de principios de uso aceptable u otros métodos apropiados.
2. Poder hacerse cumplir por medio de herramientas de seguridad, donde sea apropiado y con sanciones, donde su prevención no sea técnicamente posible.
3. Definir claramente las áreas de responsabilidad de los usuarios, administradores y directivos.

Entre los componentes que forman parte de las políticas de seguridad se incluyen:

a) el tratamiento que requiere la información oficial que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, según su categoría;
b) el empleo conveniente y seguro de las tecnologías instaladas y cada uno de los servicios que éstas pueden ofrecer;
c) la definición de los privilegios y derechos de acceso a los bienes informáticos para garantizar su protección contra modificaciones no autorizadas, pérdidas o revelación, mediante la especificación de las facultades y obligaciones de los usuarios, especialistas y directivos;
d) los aspectos relacionados con la conexión a redes de alcance global y la utilización de sus servicios;
e) el establecimiento de los principios que garanticen un efectivo control de acceso a las tecnologías (incluyen el acceso remoto) y a los locales donde éstas se encuentren;
f) las normas generales relacionadas con la información de respaldo y su conservación;
g) los principios a tener en cuenta sobre los requerimientos de Seguridad Informática que deben ser considerados en la adquisición de nuevas tecnologías;
h) los aspectos relacionados con la adquisición por cualquier vía de software y documentos de fuentes externas a la entidad y la conducta a seguir en estos casos;

i) la definición de las responsabilidades de los usuarios, especialistas y directivos, sus derechos y obligaciones con respecto a la Seguridad Informática;
j) la definición de los principios relacionados con el monitoreo del correo electrónico, la gestión de las trazas de auditoría y el acceso a los ficheros de usuario, entre otros;
k) las normas a tener en cuenta en relación con el mantenimiento, reparación y traslado de las tecnologías y del personal técnico (interno y externo) que requiere del acceso a estas por esos motivos;
l) los principios generales para el tratamiento de incidentes y violaciones de seguridad, qué se considera incidente de seguridad y a quién reportar.

Las políticas de seguridad informática son revisadas a intervalos programados o ante el surgimiento de cambios significativos para asegurar su actualización, adecuación y efectividad.

A continuación se muestran dos ejemplos de políticas:

1. El acceso a las áreas o zonas controladas se permite exclusivamente al personal autorizado.
2. El acceso a los medios informáticos es expresamente autorizado por el jefe facultado.

Obsérvese que en el primer ejemplo la política expresada limita explícitamente al personal autorizado el acceso a las áreas o zonas controladas, pero no especifica cuáles son las áreas o zonas definidas como controladas, cómo se garantiza el control en cada una de ellas, que personal es autorizado, quién está facultado para otorgar las autorizaciones, cuando se requieren estas autorizaciones y qué forma tiene la autorización (por escrito, verbal, etc.). Es aplicable en todas las áreas controladas de la entidad independientemente de su categoría (limitada, restringida o estratégica) y de la forma de su implementación en cada caso.

De igual manera en el segundo ejemplo, no se menciona cómo se realiza la autorización de los usuarios para acceder a los medios informáticos, cuando se efectúe, ni quién es la persona facultada para hacerlo.
Todas esas “aparentes insuficiencias” corresponden ser despejadas con medidas y procedimientos ajustados a las características propias de cada lugar donde corresponda aplicar esas políticas, que por supuesto no tienen por qué ser iguales en cada caso. Por ello las medidas y procedimientos sí tienen que especificar en detalle lo que hay que

hacer, pues al contrario de las políticas que están destinadas para toda la entidad, son específicas en función de las necesidades de cada área.

De lo anterior se infiere que cualquier política que se establezca necesita ser instrumentada mediante las medidas y procedimientos que garanticen su cumplimiento en cada área que lo necesite y viceversa. Debido a esto, se requiere contrastar las medidas y procedimientos que se implanten con las políticas definidas para comprobar que no existan unas sin respaldo de las otras.

1.4.2. Medidas y procedimientos de Seguridad Informática

Las medidas y procedimientos de seguridad que se implementen en correspondencia con las políticas definidas, conforman el cuerpo del sistema de seguridad diseñado y representan la línea de defensa básica de protección de los bienes informáticos, por lo que es sumamente importante su selección adecuada, de forma tal que cubran las amenazas identificadas durante el proceso de evaluación de riesgos, y se implementen de una manera rentable.

Si la mayor amenaza al sistema es un acceso remoto, tal vez no tenga mucha utilidad el empleo de dispositivos técnicos de control de acceso para usuarios locales. Por otro lado si la mayor amenaza es el uso no autorizado de los bienes informáticos por los usuarios habituales del sistema, probablemente es necesario establecer rigurosos procedimientos de monitoreo y de gestión de auditoría.

Las medidas y procedimientos que se establecen son definidos de manera suficientemente clara y precisa, para evitar interpretaciones ambiguas por parte de los responsabilizados con su cumplimiento.

La seguridad es implementada mediante el establecimiento de múltiples barreras de protección, la selección de controles de diferentes tipos de forma combinada y concéntrica, para lograr con ello una determinada redundancia que garantice que si una medida falla o resulta vulnerada, la siguiente medida entre en acción y continúe la protección del activo o recurso. No es conveniente que el fallo de un solo mecanismo comprometa totalmente la seguridad.

La implementación de múltiples medidas simples puede en muchos casos ser más seguro que el empleo de una medida muy sofisticada. Esto cobra mayor validez cuando determinada medida no puede ser aplicada por alguna limitación existente, como pueden

ser, por ejemplo: las insuficiencias del equipamiento, que impiden la implementación de una medida técnica. En este caso son consideradas medidas o procedimientos complementarios de otro tipo, que garanticen un nivel de seguridad adecuado.

Hay que tener en cuenta también que el uso del sentido común y una buena gestión son las herramientas de seguridad más apropiadas. De nada vale diseñar un sistema de medidas muy complejo y costoso si se pasan por alto los controles más elementales. Por ejemplo, independientemente de cuán sofisticado sea un sistema de control de acceso, un simple usuario con una clave pobre o descuidada puede abrir las puertas del sistema.

Otro elemento importante a considerar al implementar las medidas y procedimientos es aplicar el principio de proporcionalidad o racionalidad, que consiste en ajustar su magnitud al riesgo presente en cada caso. Por ejemplo, la salva de la información puede tener diferentes requerimientos en distintas áreas y en una misma área para distintos tipos de datos o programas.

Las medidas de Seguridad Informática se clasifican de acuerdo con su origen en: administrativas; de seguridad física, técnica o lógica; de seguridad de operaciones; legales y educativas. A su vez, por su forma de actuar, las medidas pueden ser: preventivas, de detección y de recuperación.

Medidas administrativas

Las medidas administrativas, frecuentemente no son apreciadas en toda su importancia, a pesar de que la práctica ha demostrado que un elevado por ciento de los problemas de seguridad se puede evitar con medidas de esta naturaleza.

Se establecen por la dirección de cada entidad mediante las regulaciones comprendidas dentro de sus facultades y por tanto, son de obligatorio cumplimiento por todo el personal hacia el cual están dirigidas.

Medidas de seguridad física

Constituyen la primera barrera de protección en un Sistema de Seguridad Informática e introducen un retardo que incrementa el tiempo de materialización de un acto doloso o accidental.

Se aplican a los locales donde se encuentran las tecnologías de información y directamente a estas mismas tecnologías e incluyen: medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.

Medidas técnicas o lógicas

Son las de mayor peso dentro de un sistema de Seguridad Informática. Pueden ser implementadas por software, a nivel de sistemas operativos y de aplicaciones o por hardware. El uso combinado de técnicas de software y hardware aumenta la calidad y efectividad en la implementación de este tipo de medidas.

Algunos tipos de medidas técnicas son empleadas para identificar y autentificar usuarios, protección criptográfica, protección contra virus y otros programas dañinos y registro de auditoría, entre otros.

Medidas de seguridad de operaciones

Están dirigidas a lograr una eficiente gestión de la seguridad mediante la ejecución de procedimientos definidos y garantizan el cumplimiento de las regulaciones establecidas por cada entidad y por las instancias superiores a esta.

Medidas legales

Representan un importante mecanismo de disuasión que contribuye a prevenir incidentes de seguridad y sancionar adecuadamente a los violadores de las políticas establecidas por la entidad.

Se establecen mediante disposiciones jurídicas y administrativas, en las que se plasman: deberes, derechos, funciones, atribuciones y obligaciones, así como se tipifican las violaciones y tipos de responsabilidad administrativas, civiles, penales u otras.

Medidas educativas

Están dirigidas a inculcar una forma mental de actuar, mediante la cual el individuo esté consciente de la existencia de un Sistema de Gestión de la Seguridad Informática en el que le corresponde una forma de actuar. Se sustentan en dos elementos fundamentales:

1. La existencia de un Sistema de Gestión de la Seguridad Informática.

2. La participación consciente del hombre en el éxito de los objetivos de seguridad planteados.

Medidas de recuperación

Están dirigidas a garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos ante cualquier eventualidad que pueda ocurrir, que afecte o ponga en peligro su normal desarrollo.

Se establecen a partir de la identificación de los posibles incidentes o fallas que puedan causar la interrupción o afectación de los procesos informáticos y garantizan las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios para ello.

Procedimientos de Seguridad Informática

La implementación de las políticas de seguridad informática requiere generalmente la realización de un conjunto de acciones para garantizar su cumplimiento. La descripción de esta secuencia de acciones constituye un procedimiento de seguridad. Los procedimientos, al igual que las medidas, se clasifican en procedimientos de prevención, de detección y de recuperación.

Los **procedimientos de prevención** tienen el objetivo de asegurar las acciones que se requieren para evitar que una amenaza se materialice y los **de detección** se dirigen a identificar cualquier tipo de indicio que revele la posible materialización de una amenaza, una amenaza en desarrollo o una vulnerabilidad en los sistemas.

La función de los **procedimientos de recuperación**, por el contrario, no es la de prevenir ni la de detectar la materialización de determinadas amenazas, sino la de establecer las acciones que se ejecutan cuando una amenaza ya se ha materializado y afectan parcial o totalmente los bienes informáticos.

En el desarrollo de los procedimientos se usa un lenguaje preciso y una cuidadosa redacción y quedan claras las ideas principales, de forma tal que resulten comprensibles a quienes corresponda su aplicación. Los procedimientos son autosuficientes.

La importancia del establecimiento de procedimientos correctamente definidos garantiza, además de la uniformidad en la aplicación de las políticas, la seguridad de su

cumplimiento y su sistematicidad. Algunos procedimientos de seguridad que pueden ser implementados son:

a) De administración de cuentas de usuarios;
b) de asignación y cancelación de permisos de acceso a las tecnologías y sus servicios;
c) de asignación y cancelación de derechos y privilegios;
d) de gestión de incidentes;
e) de gestión de contraseñas;
f) de gestión de salvas;
g) de realización de auditorías;
h) de acceso a las áreas;
i) de entrada y salida de las tecnologías y sus soportes.

Ejemplo de una política y de algunas medidas y procedimientos para su implementación.

Política: "La información es salvada en soportes magnéticos u ópticos con la periodicidad requerida en cada caso, a fin de garantizar su restablecimiento en caso de incidentes de seguridad".

Medidas:

1. La información que se comparte en los servidores de la red se salva en los casetes de cinta habilitados al efecto, diariamente en dos versiones.
2. Las bases de datos de contabilidad son salvadas en discos reescribibles en dos versiones. Diariamente se salvan las modificaciones realizadas y mensualmente toda la información.

Procedimientos:

a) En los servidores:

1. Realizar la salva de la información que se comparte en los servidores en dos casetes numerados, se alternan diariamente, una hora antes de concluir la jornada de trabajo. Utilizar el casete marcado con el No. 1 los días impares y con el No. 2 los días pares.
   Responsable: Administrador de la red

2. Anotar en el modelo de registro establecido (anexo N) la fecha, la hora y el casete utilizado.
   Responsable: Administrador de la red
3. Verificar integridad de la información salvada.
   Responsable: Jefe de Departamento de Redes
4. Guardar la salva bajo llave en el archivo metálico ubicado en la oficina del Jefe del Departamento de Redes.
   Responsable: Jefe del Departamento de Redes

b) En el Departamento de Contabilidad:

1. Realizar la salva de las bases de datos en discos compactos, se alternan diariamente, al finalizar la jornada de trabajo y el último día hábil de cada mes. Los discos para la salva diaria están marcados con una franja, se utilizan los de la franja roja para los días impares y los de la franja azul para los días pares. Los discos para la salva mensual son numerados del 1 al 12 en correspondencia con cada mes.
   Responsable: Administrador de la aplicación
2. Anotar en el modelo de registro establecido (anexo M) la fecha, la hora y el disco utilizado.
   Responsable: Administrador de la aplicación
3. Verificar integridad de la información salvada.
   Responsable: Jede de Departamento de Contabilidad
4. Guardar la salva bajo llave en el archivo metálico ubicado en la oficina del Jefe del Departamento de Contabilidad.
   Responsable: Jefe del Departamento de Contabilidad

1.5. Organización de la Seguridad Informática

Con el objetivo de gestionar la seguridad informática se establece un marco apropiado para iniciar y controlar su implementación dentro de la organización.

1.5.1. Organización interna

La dirección aprueba las políticas de seguridad informática de la entidad, asigna roles de seguridad, coordina y revisa la implementación de la seguridad a través de la organización.

Si es necesario, gestiona una fuente de asesoramiento especializada en seguridad informática. Son establecidos contactos con especialistas de seguridad o grupos externos a la organización, incluyen autoridades pertinentes, para mantenerse al día con tendencias de la industria, seguimiento de normas, métodos de evaluación y proveer puntos de enlace adecuados cuando se deban manejar incidentes de seguridad informática. Se propicia un enfoque multidisciplinario hacia la seguridad informática.

1.5.2. Coordinación de la Seguridad Informática

Las actividades referentes a la seguridad informática son coordinadas por los Consejos de Dirección de los órganos, organismos y entidades, que pueden incluir personal de diferentes partes de la organización con funciones y roles específicos. Esta coordinación:

a) asegura que las actividades referentes a la seguridad son ejecutadas de acuerdo a las políticas establecidas;
b) identifica cómo manejar los incumplimientos;
c) aprueba metodologías y procedimientos para la seguridad informática, por ejemplo, de evaluación de riesgos, respaldo de la información y tratamiento de incidentes;
d) identifica cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas;
e) evalúa la adecuación y coordinación de la implementación de los controles de seguridad informática;
f) promueve en forma efectiva la educación, la formación y la concienciación en seguridad informática a través de la organización;
g) evalúa la información resultante del tratamiento y análisis de los incidentes de seguridad informática y las acciones recomendadas en su respuesta.

1.5.3. Asignación de responsabilidades sobre Seguridad Informática

Se definen las responsabilidades de seguridad informática del personal vinculado con el sistema informático de acuerdo con su participación en este. La asignación de las responsabilidades de seguridad informática se hace en correspondencia con las políticas de seguridad informática, se definen claramente las responsabilidades asociadas con la protección de los bienes informáticos y para la ejecución de procesos específicos de seguridad, como por ejemplo, la gestión de incidentes. Estas responsabilidades son complementadas, de ser necesario, con medidas y procedimientos específicos.

Las personas con responsabilidades de seguridad asignadas pueden delegar tareas de seguridad a otras, sin embargo, mantienen la responsabilidad y garantizan que cualquier tarea delegada se ha cumplido correctamente. Se establecen claramente las áreas de las cuales los individuos son responsables. En particular se considera lo siguiente:

a) definir y documentar los niveles de autorización;
b) identificar y definir los bienes informáticos y los procesos de seguridad asociados con cada sistema específico;
c) asignar el responsable de cada bien informático o proceso de seguridad y documentar los detalles de dicha responsabilidad.

Se asegura que cada cual conozca su responsabilidad en relación con el mantenimiento de la seguridad y que cada clase de problema tenga alguien asignado para tratarlo; y se involucra a todo el personal relacionado con los bienes informáticos. Por ejemplo, los usuarios son responsables del uso adecuado de sus identificadores y contraseñas y los administradores de redes y sistemas están obligados a cubrir las brechas de seguridad y corregir los errores. Para alcanzar una seguridad efectiva es conveniente lograr una participación lo más amplia posible de todo el personal (o al menos la ausencia de una oposición activa).

Se establecen niveles de responsabilidad asociados con las políticas de seguridad. Por ejemplo, en una red se puede definir un nivel con sus usuarios, donde cada uno tiene la responsabilidad de proteger su cuenta. Un usuario que permita que su cuenta sea comprometida incrementa la posibilidad de comprometer otras cuentas o recursos. Los administradores de redes y sistemas forman otro nivel de responsabilidad; se implementan los mecanismos de seguridad que se requieran.

Queda claro que los usuarios son individualmente responsables de la comprensión y aplicación de las políticas de seguridad de los sistemas que ellos emplean y del uso apropiado de los recursos que les han sido asignados.

1.6. Elaboración del Plan de Seguridad Informática

Una vez cumplidas las actividades anteriores, el siguiente paso es la elaboración del Plan de Seguridad Informática, en lo adelante PSI como constancia documentada del Sistema de Seguridad Informática diseñado y constituye el documento básico que recoge claramente las responsabilidades de cada uno de los participantes en el proceso

informático y establece los controles que permiten prevenir, detectar y responder a las amenazas que gravitan sobre el sistema informático de cada entidad.

El objetivo del PSI es establecer los requisitos de seguridad del sistema y en él se especifican los controles previstos en cada área o lugar para cumplirlos. El PSI también describe las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema y refleja las contribuciones de los distintos actores con responsabilidades sobre el SGSI.

En el PSI se refiere **cómo** se implementan, en las áreas a proteger, las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, de acuerdo con sus formas de ejecución, periodicidad, personal participante y medios**.**

Se particularizan en el PSI los controles de seguridad implementados en correspondencia con su naturaleza, de acuerdo con el empleo que se haga de los recursos humanos, de los medios técnicos o de las medidas y procedimientos que cumple el personal. **En la Segunda Parte: Estructura y contenido del Plan de Seguridad Informática** se refieren con mayor detalle los elementos necesarios para la elaboración del PSI.

2. Proceso de Implementación del SGSI

Objetivo principal: garantizar una adecuada implementación de los controles seleccionados y su correcta aplicación.

Durante el proceso de implementación del SGSI se comienzan a gestionar los riesgos identificados mediante la aplicación de los controles seleccionados y las acciones apropiadas por parte del personal definido (recursos humanos), los recursos técnicos disponibles en función de la seguridad (medios técnicos) y las medidas administrativas, que garanticen la implantación de controles efectivos para lograr el nivel de seguridad necesario, en correspondencia con los objetivos de la organización, de manera que se mantenga siempre el riesgo por debajo del nivel asumido por la propia entidad.

Se garantiza que el personal al que se asignen responsabilidades definidas en el SGSI esté en capacidad de realizar las tareas exigidas, mediante la formación y el entrenamiento que les permita adquirir el conocimiento y las habilidades que requieran, en correspondencia con su papel dentro del sistema, para lo que se implementan programas de capacitación.

La organización también asegura que el personal tiene conciencia de la necesidad e importancia de las actividades de seguridad informática que le corresponde realizar y cómo ellas contribuyen al logro de los objetivos del SGSI.

Las actividades de formación y sensibilización incluyen:

1. Concienciar al personal de la importancia que el SGSI tiene para la organización.
2. Garantizar la divulgación, el conocimiento y comprensión de las políticas de seguridad que se implementan.
3. Capacitar a los usuarios en las medidas y procedimientos que se van a implantar.
4. Lograr que el personal esté consciente de los roles a cumplir dentro del SGSI.

Se requiere además precisar el procedimiento de medición de la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se van a emplear estas mediciones, con la finalidad de evaluar su eficacia para producir resultados comparables y reproducibles y de esta forma, determinar si las actividades de seguridad implementadas satisfacen las expectativas concebidas.

Finalmente se implementan los procedimientos y controles que se requieran para detectar y dar respuesta oportuna a los incidentes de seguridad que se presenten, que incluyen su reporte a las instancias pertinentes.

El proceso de implementación es una etapa crucial del SGSI y tal vez la más difícil. De nada vale haber realizado una buena determinación de las necesidades de protección e incluso haber hecho una excelente selección de los controles de seguridad a aplicar, si no se logra implantarlos en cada lugar, se ajustan a las particularidades de los bienes a proteger y a las exigencias específicas de cada área.

Se puede haber definido, por ejemplo, una refinada política de respaldo de la información en previsión de cualquier tipo de contingencia que pudiera presentarse, y no implementar los procedimientos que determinen con exactitud qué información es preservada; con qué frecuencia se salva, en qué soporte y en cuantas copias; quienes están encargados de ejecutar esas acciones y como se garantiza su protección y conservación, de manera que exista la certeza de su integridad cuando requieran ser utilizadas.

Puede haberse confeccionado un Plan de Seguridad Informática que cumpla a cabalidad los requisitos metodológicos, pero en sus partes esenciales se queda “en el papel” y no se

conoce ni se aplica por los que tienen que instrumentar los controles que fueron definidos. Por ejemplo, en ocasiones se especifica en el plan la estructura y fortaleza de las contraseñas de acceso a la red y sin embargo, no se configuran en el servidor las reglas que en correspondencia con lo establecido obliguen a los usuarios a su cumplimiento.

De igual forma, pueden haberse concebido los procedimientos para otorgar o cancelar el acceso a sistemas y servicios pero estos no se conocen o se incumplen por los que tienen que ejecutarlos regularmente. Ejemplos semejantes pueden referirse en relación con la gestión de parches de seguridad, la seguridad de las redes inalámbricas, el control de los soportes removibles, la gestión de incidentes y el análisis y conservación de los registros generados por los sistemas y servicios, por solo citar algunos de los más comunes.

De modo que el proceso de implementación del SGSI para que sea exitoso garantiza la implantación de todos los controles que fueron concebidos y su conocimiento y comprensión por los encargados de ejecutarlos y cumplirlos.

2.1. Programa de Desarrollo de la Seguridad Informática

Puede ser que la implementación de algunos controles requiera de un tiempo adicional, ya sea porque necesitan algún tipo de recursos con que no se cuenta, la realización de gestiones complementarias u otras causas. Las acciones que sean necesarias para lograr la implementación de estos controles se incluyen en un programa que señala los plazos para su cumplimiento y el personal responsabilizado con su ejecución. Los aseguramientos que se deriven de estas acciones son considerados dentro del Plan de Inversiones de la entidad cuando se requiera. El cumplimiento de este programa contribuye al proceso de mejora continua del SGSI y es actualizado según se ejecute. Algunos aspectos a considerar al elaborar el Programa de Desarrollo de la Seguridad Informática pudieran ser los siguientes:

1. La implementación a mediano y largo plazo de aquellos aspectos que así lo exijan para alcanzar un mayor nivel de seguridad, como por ejemplo la introducción de medios técnicos de seguridad, modificación de locales, etc.
2. La preparación y capacitación del personal en materia de seguridad informática, según su participación en el sistema diseñado, ya sea a través de cursos específicos, mediante la impartición de materias relacionadas con el tema y con acciones de divulgación.

3. La organización y ejecución de controles, inspecciones y auditorías (internas y externas), mencionan con qué frecuencia se realizan, quienes participan y su contenido.

2.2 Factores Críticos de éxito

La implementación exitosa de los controles seleccionados y su correcta aplicación en una organización presupone, además, la consideración de los factores siguientes:

a) La política de seguridad, objetivos y actividades que reflejen los intereses de la organización;
b) el enfoque para implantar la seguridad que sea consistente con la cultura de la organización;
c) el apoyo visible y el compromiso de la alta dirección;
d) la buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo;
e) la comunicación eficaz de la necesidad de la seguridad a todos los directivos y trabajadores;
f) la distribución a todos los trabajadores de directrices y normas sobre la política de seguridad informática de la organización;
g) suministrar recursos para las actividades de gestión de la seguridad informática;
h) proporcionar concienciación, formación y educación apropiadas;
i) proceso efectivo de gestión de incidentes de seguridad informática;
j) implementación de un sistema de medición para evaluar el desempeño en la gestión de seguridad informática y las sugerencias de mejoras.

Durante el proceso de implementación del SGSI es necesario precisar la aplicación de cada uno de los controles seleccionados en las áreas que los requieren y que cubran los riesgos que para ellas fueron identificados. En este sentido, la participación de los jefes de áreas es determinante, pues corresponde a ellos refrendar que los controles que se establezcan dan plena respuesta a los requerimientos de protección de cada área en particular.

Para cumplir con lo expresado en el párrafo anterior se elabora un cronograma de implementación por áreas, mediante el cual los jefes de estas garanticen:

1. La concienciación del personal sobre la necesidad e importancia de sus actividades de Seguridad Informática y cómo ellas contribuyen al logro de los objetivos del SGSI.

2. La preparación del personal para el cumplimiento de sus obligaciones en cuanto a la Seguridad Informática.
3. La implantación de los controles de seguridad, tanto los comunes para toda la entidad como los específicos para el área.
4. La verificación de que los controles aplicados garantizan el cumplimiento de las políticas de seguridad establecidas en la organización.
5. La precisión de los métodos de evaluación de la eficacia de los controles que se implementen.
6. La identificación de los controles que no es posible implantar y deban ser incluidos en el Programa de Desarrollo de la Seguridad Informática.

No se puede dar por terminado el proceso de implementación del SGSI por el dirigente máximo de la entidad, hasta que en todas las áreas sus Jefes acrediten el cumplimiento de estos requisitos.

3. Proceso de Verificación del SGSI

Objetivo principal: Revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
Uno de los aspectos más importantes en el proceso de diseño e implementación de un SGSI es el establecimiento de los indicadores y métricas de gestión. Esto permite a la Dirección valorar si los esfuerzos realizados cumplen o no con los objetivos planteados. Para ello se utiliza la medición como instrumento de control. Es necesario lograr diagnosticar correctamente qué pasa y qué es necesario corregir para poder gestionar.

Mediante el proceso de revisión se comprueba la conformidad con los patrones establecidos y como parte de ello se mide el rendimiento y la eficacia del SGSI, para lo cual se precisa considerar las acciones siguientes:

1. Revisiones periódicas de los indicadores seleccionados.
2. Revisiones de los riesgos residuales y riesgos aceptables.
3. Realización de auditorías internas/externas del SGSI.
4. Comunicación de los resultados de las auditorías a las partes interesadas.

La ejecución de procedimientos de revisión mediante instrumentos de medición posibilita detectar errores de proceso, identificar fallos de seguridad de forma rápida y determinar las acciones a realizar. Se utilizan para ello los indicadores seleccionados sobre la base de los criterios en relación a qué aspectos se controlan y miden para lograr el cumplimiento de las metas planteadas.

Los objetivos de estos procedimientos de revisión son:

1. Evaluar la efectividad de la implementación de los controles de seguridad.
2. Evaluar la eficiencia del SGSI, incluyen mejoras continuas.
3. Proveer estados de seguridad que guíen las revisiones del SGSI, faciliten mejoras a la seguridad y nuevas entradas para auditar.
4. Comunicar valores de seguridad a la organización.
5. Servir como entradas al análisis y tratamiento de riesgos.

La gestión del Sistema de Seguridad Informática se basa en un ciclo de mejora continua, por lo que es vital medir para poder observar cómo las cosas mejoran a medida que el sistema madura. Si no se mide, se trabaja en base a sensaciones, y las decisiones tomadas sin la información necesaria pueden conducir a equivocaciones.
Pasado el tiempo previsto de antemano, hay que volver a recopilar datos de control y analizarlos, compararlos con los objetivos y especificaciones iniciales, para evaluar si se han producido cambios que afecten los resultados esperados. Donde sea aplicable, se mide el desempeño del SGSI contra las políticas y los objetivos de seguridad y la experiencia práctica, y se reporta los resultados a la Dirección, para su revisión.

3.1. Métodos de Medición

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicarse a múltiples aspectos. Por su naturaleza, los métodos de medición pueden ser subjetivos u objetivos. Los métodos subjetivos implican el criterio humano, mientras que los objetivos se basan en una regla numérica, que puede ser aplicada por personas o recursos automatizados. Algunos ejemplos de métodos de medición son:

1. Encuestas/indagaciones.
2. Observación.
3. Entrevistas
4. Cuestionarios.
5. Evaluación de conocimientos.
6. Inspecciones.
7. Consulta a sistemas.
8. Supervisión
9. Muestreo.

Para la implementación de estos métodos en cualquier entidad hay disponibles diferentes procedimientos y herramientas que facilitan esta tarea, entre ellas:

1. Utilización de listas de verificación de la conformidad del SGSI con aspectos normados que requieren cumplirse.
2. La aplicación de programas diseñados con este objetivo, como por ejemplo el sistema de evaluación Diógenes elaborado por la Oficina de Seguridad para las Redes Informáticas.
3. La realización de diagnósticos de seguridad presenciales y remotos por especialistas de la propia organización o contratados a terceros.
4. La evaluación de los resultados obtenidos del análisis de los registros de auditoría generados por sistemas y servicios.
5. El análisis de los resultados de la supervisión del empleo de los sistemas y servicios por parte de los usuarios autorizados para ello.
6. Los reportes y alarmas generados por los sistemas de seguridad, como por ejemplo un Sistema de Detección de Intrusos (IDS por sus siglas en inglés).
7. El análisis de los incidentes de seguridad ocurridos a partir de la información registrada sobre estos.
8. El análisis de los reportes de las violaciones de los controles de seguridad.
9. El análisis de las no conformidades detectadas en controles realizados y su erradicación.

La medición sirve para cuestionar continuamente en base a datos y registros, si los controles de seguridad funcionan bien. Se establece un conjunto de indicadores que sirven para evidenciar que lo implementado funciona correctamente.

3.2. Indicadores de medición

En esta etapa adquieren especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI.

Cada indicador tiene asociado valores que representen las metas a cumplir. En este sentido, cada organización define su criterio respecto a qué aspectos quiere controlar y medir para lograr el cumplimiento de los objetivos. Para ello se pueden definir distintos grupos de indicadores que recojan los diferentes ámbitos que se quieren gestionar. Por tanto, se podrían tener:

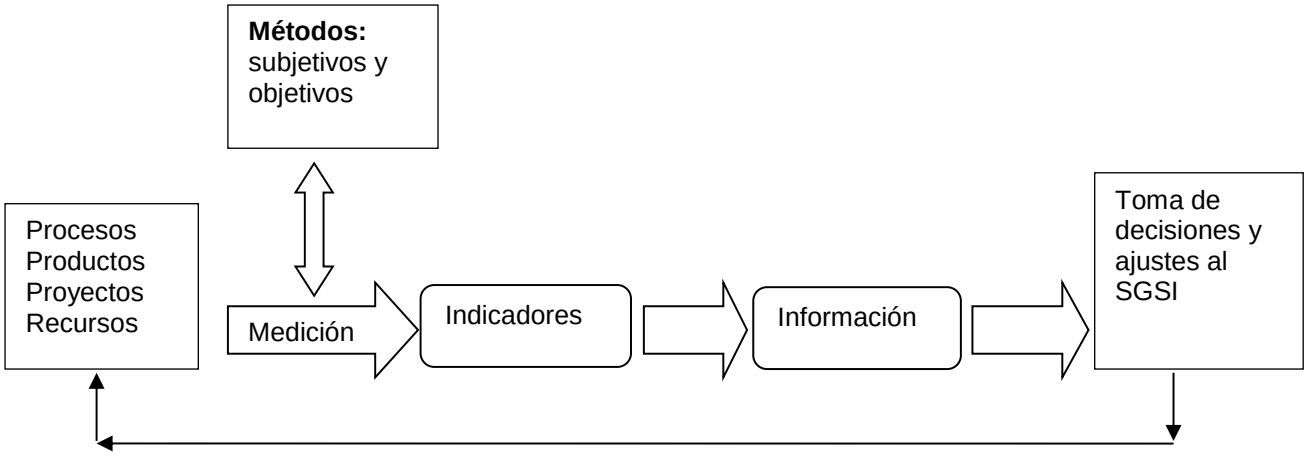
1. **Indicadores del grado de efectividad de los controles de seguridad:** Su sentido es valorar si los controles implantados funcionan bien o es necesario ajustarlos.
2. **Indicadores de medición del entorno y la hostilidad:** Su misión es detectar cambios en el entorno y contexto que rodea al SGSI para realizar ajustes respecto al análisis de riesgos por aparición de nuevas amenazas o cambios en sus

frecuencias de ocurrencia. Por ejemplo, la aparición de nuevas amenazas internas, cambios en el clima laboral de la organización, frecuencia de publicación de vulnerabilidades, detección de nuevas aplicaciones malware.

3. **Indicadores de gestión interna:** Estos se establecen para evaluar el funcionamiento propio del propio SGSI y tiene que ver con la monitorización de las tareas propias de gestión. Por ejemplo, las relacionadas con la eliminación en plazo de no conformidades, el porcentaje de cumplimiento de los objetivos planteados, el número de no conformidades detectadas por auditoría.

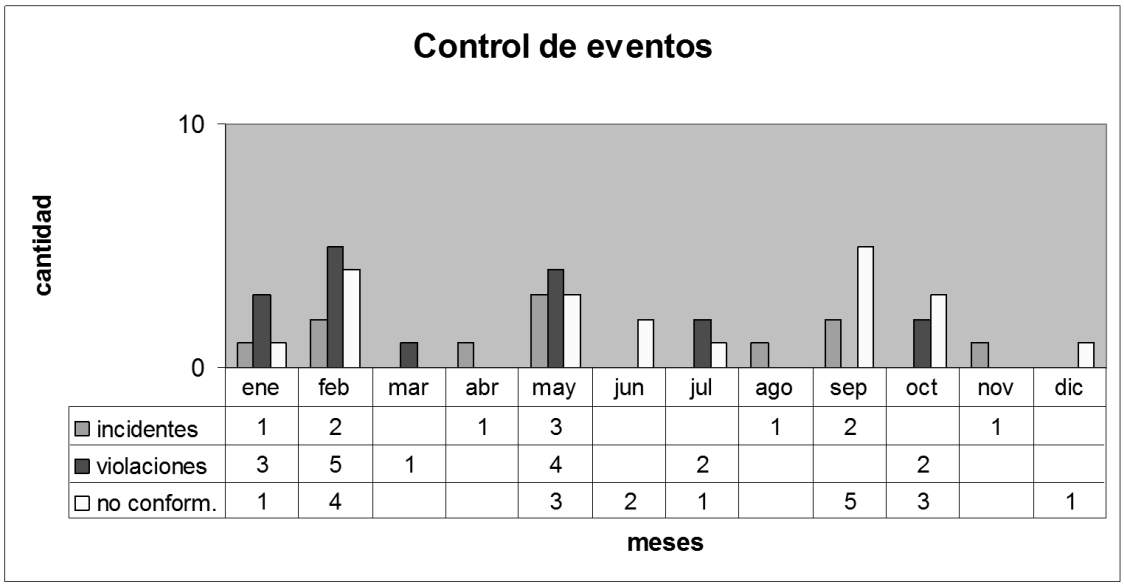
Al definir y valorar el comportamiento de los indicadores, se tiene muy en cuenta el daño derivado de la ocurrencia de un incidente y su posible impacto en los objetivos de la organización.

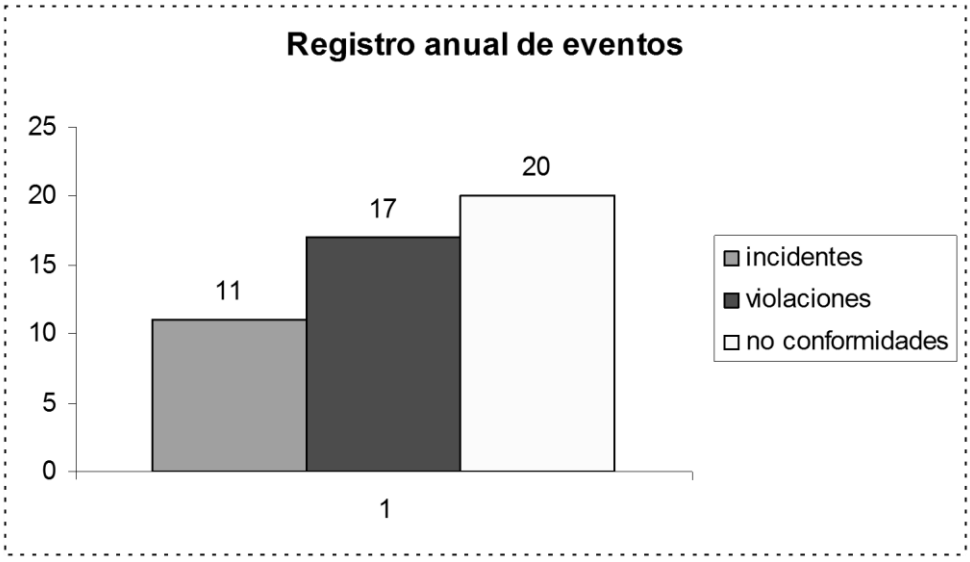
La información referente a estos indicadores, desde la perspectiva de la gestión, es la más crítica, dado que es la base de la retroalimentación del sistema. Por tanto, hay que disponer de sensores de diferente naturaleza y con diferentes objetivos: medir la evolución de la ejecución del plan, valorar el rendimiento y funcionamiento de las medidas de seguridad, vigilar el entorno por si se vuelve más hostil y otros.



Al final lo importante es no perder el sentido del por qué se hacen las cosas. Para ello, toda esta información se transforma en unas sencillas gráficas que la Dirección pueda entender y que sirvan como el auténtico "termómetro de la situación". Estos datos, adecuadamente procesados y visualmente representados, sin disponer de excesivos detalles y conocimientos técnicos, permiten a la Dirección realizar su principal labor dentro del SGSI: tomar decisiones y realizar los ajustes necesarios para el logro de los objetivos.

A modo de ejemplo se muestra a continuación una tabla y un gráfico con datos de tres indicadores seleccionados:





Otro aspecto a tener en cuenta es el de la frecuencia. Se definen y programan claramente los intervalos en los cuales se lleva a cabo cada medición (semanal, mensual, trimestral, anual y otros.), se considera una relación entre la necesidad de contar con esta información y el esfuerzo para obtenerla (costo/beneficio).

Se puede definir un total de factores a evaluar (que nombraremos como K) y ver cuántos de ellos se cumplen (que nombraremos como k).

Por ejemplo: De 10 factores predeterminados se cumplen 7

K = 10 y k = 7
7/10 = 0.7 => 70 %

Algunas posibles relaciones para indicadores pudieran ser:

a) tiempo sin interrupciones/Tiempo total de servicio;
b) tiempo sin violaciones reportadas/Tiempo total de servicio;
c) 1/cantidad de incidentes computacionales;
d) velocidad real/velocidad contratada;
e) no conformidades detectadas/total de aspectos verificados.

3.3. Reglas que cumple una buena métrica:

1. Ser objetivas: aportan un criterio de recogida de datos medible y objetivo, que no dependa de valoraciones subjetivas.
2. Ser fáciles de obtener: Los datos sencillos, simples de calcular y poco costosos de recoger son buenos candidatos a ser métricas. Al respecto, lo más sencillo es recurrir a datos proporcionados por herramientas o procesados de forma automatizada.
3. Expresables de forma numérica o porcentual. No se basan en etiquetas cualitativas tales como "alto", "medio" o "bajo".
4. Expresable con el uso de algún tipo de unidad de medida: Siempre están vinculadas a algo tangible basado en escalas como el tiempo, número de defectos, o cuantías económicas.
5. Significativas: Toda buena métrica es significativa, es relevante para el hecho o circunstancia que se desea medir y aporta criterio. Una métrica que no aporta información no es una buena métrica y es desechada.

4. Proceso de Actualización del SGSI

Mantenimiento, mejora y corrección del SGSI

Objetivo principal: Realizar los cambios que sean necesarios para mantener el máximo rendimiento del SGSI

El proceso de actualización del SGSI comprende la aplicación de acciones correctivas y preventivas, basadas en los resultados del proceso de verificación descrito en el apartado anterior, para lograr la mejora continua.

En esta etapa se llevan a cabo las labores de mantenimiento del sistema, así como las acciones de mejora y de corrección identificadas si, tras la verificación, se ha detectado algún punto débil. Este proceso se suele llevar en paralelo con la verificación y se actúa al detectarse la deficiencia, no se espera a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

El SGSI se mantiene eficiente durante todo el tiempo y se adapta a los cambios internos de la organización, así como los externos del entorno. Para lograr el perfeccionamiento constante del SGSI se aplican las lecciones aprendidas de las experiencias de seguridad de otras organizaciones, las de la propia entidad y la de los incidentes ocurridos.

Durante la Implementación de los resultados derivados de la verificación se requiere, generalmente, modificar controles e implantar las mejoras identificadas en las revisiones del SGSI a partir de las decisiones sobre los cambios requeridos para mejorar el proceso y en consecuencia se:

1. Estandarizan los cambios de procesos.
2. Comunican los cambios a todos los implicados.
3. Proporciona entrenamiento al personal sobre los nuevos métodos.
4. Evalúan los nuevos riesgos.
5. Modifica el SGSI.
6. Actualiza el PSI.

Se comunican las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias, se precisa sobre cómo proceder ante el nuevo escenario y se entrena al personal con el fin de asegurar que las mejoras logren los objetivos previstos.

Algunos ejemplos de circunstancias que implican la necesidad de un nuevo análisis de riesgos pudieran ser las siguientes:

1. Instalación de nuevos tipos de redes (por ejemplo una red inalámbrica) en áreas de la entidad o de algún nuevo enlace para la comunicación con otras instancias.
2. Cambios en la topología de las redes o en la arquitectura de seguridad.

3. Introducción de tecnologías que no se habían empleado con anterioridad.
4. Incremento del empleo de soportes removibles como portadores de información por parte del personal.
5. Ocurrencia de algún incidente de seguridad.
6. Puesta en marcha de una nueva aplicación o introducción de un nuevo servicio de red.
7. Nuevos requerimientos informativos para la organización.
8. Incorporación de personal con poca experiencia y conocimientos.
9. Cambios en la plantilla de personal, en su composición o completamiento.
10. Conversión de locales de uso interno en áreas de acceso público.
11. Modificaciones estructurales de los inmuebles o cambios en su distribución.

Una vez realizados los cambios necesarios para mantener el máximo rendimiento del SGSI, se actualiza el PSI en las partes que corresponda e informan de ello a todos los que requieran conocerlo.

Segunda Parte: Estructura y contenido del Plan de Seguridad Informática

Consideraciones Generales

Para la elaboración del Plan de Seguridad Informática se tienen en cuenta las consideraciones siguientes:

1. El PSI es un documento de trabajo y como tal es accesible a todo el personal que requiera su utilización, por lo que la información que en él se incluye es ordinaria. No se incluye en este, información limitada o clasificada, la cual, de ser necesario, forma parte de un documento independiente que es categorizado conforme con lo establecido en la legislación vigente en materia de seguridad y protección de la información oficial.

2. El PSI se ajusta en todo momento al sistema de seguridad diseñado e implementado, se evitan formalismos y definiciones conceptuales y se utilizan como una herramienta de trabajo para la gestión de la seguridad.

3. Su redacción es simple, clara y libre de ambigüedades para que sea comprensible por todos los involucrados en su cumplimiento.

4. Tiene un carácter impositivo por lo que se evitan términos tales como “se recomienda”, “se debe” y otros similares que no implican obligatoriedad.
5. Contiene las tablas, gráficos y otros complementos que contribuyan a su mejor interpretación.

6. Se mantiene permanentemente actualizado sobre la base de los cambios que se produzcan en las condiciones consideradas durante su elaboración.

Presentación del Plan de Seguridad Informática

La página inicial (portada) contiene el título siguiente: “**PLAN DE SEGURIDAD INFORMATICA**” seguido de la denominación de la entidad. En la segunda página se consignan los datos referidos a la elaboración, revisión y aprobación del Plan de Seguridad Informática, de acuerdo con el formato siguiente:

	Elaborado	**Revisado**	**Aprobado**
Nombre			
Cargo			
Firma			
Fecha			

En la columna “**elaborado**” se consignan los datos de la persona que dirigió el equipo que confeccionó el Plan de Seguridad Informática, en la columna “**revisado**” los de la persona designada para su revisión antes de presentarlo a aprobación y en la columna “**aprobado**” se reflejan los datos del jefe de la entidad en la que el Plan tiene vigencia.

Estructura del Plan de Seguridad Informática

Los componentes del PSI se estructuran de la forma siguiente:

1. Alcance del PSI.
2. Caracterización del Sistema Informático.
3. Resultados del análisis de riesgos.
4. Políticas de Seguridad Informática.
5. Responsabilidades.
6. Medidas y Procedimientos de Seguridad Informática
   6.1. Clasificación y control de los bienes informáticos.
   6.2. Del Personal.

6.3. Seguridad Física y Ambiental.
6.4. Seguridad de Operaciones.
6.5. Identificación, Autenticación y Control de Acceso.
6.6. Seguridad ante Programas Malignos.
6.7. Respaldo de la Información.
6.8. Seguridad en Redes.
6.9. Gestión de Incidentes de Seguridad.

7. Anexos del Plan de Seguridad informática.
7.1. Listado nominal de usuarios.
7.2. Registros.
7.3. Control de cambios.

1. Alcance del Plan de Seguridad Informática

El primer asunto que se define en el PSI es su espacio de aplicación, o sea su alcance. El alcance expresa el radio de acción que abarca el Plan, de acuerdo con el Sistema Informático objeto de protección, para el cual fueron determinados los riesgos y diseñado el Sistema de Seguridad. La importancia de dejar definido claramente el alcance del Plan (y de ahí su inclusión al comienzo de este) consiste en que permite tener, a priori, una idea precisa de la extensión y los límites en que este tiene vigencia.
A modo de ejemplo, la definición del alcance del PSI en una entidad hipotética (Empresa X) podría ser:

"El presente Plan de Seguridad Informática es aplicable en su totalidad en las áreas de la Oficina Central de la Empresa X que se encuentran en el edificio situado en la calle Martí No. 610, entre Céspedes y Agramonte, La Habana.
Las políticas expresadas en este plan son de obligatorio cumplimiento para todo el personal de la Empresa X, incluyen los de sus dependencias que se encuentran en los municipios Plaza, Playa y Cerro".

2. Caracterización del Sistema Informático

Se describe de manera detallada el sistema informático de la entidad, precisan los elementos que permitan identificar sus particularidades y las de sus principales componentes: la información, las tecnologías de información, las personas y los inmuebles, y se considera entre otros:

1. Bienes informáticos, su destino e importancia.

2. Redes instaladas, estructura, tipo y plataformas que utilizan.
3. Aplicaciones en explotación.
4. Servicios informáticos y de comunicaciones disponibles.
5. Características del procesamiento, transmisión y conservación de la información, se tiene en cuenta el flujo interno y externo y sus niveles de clasificación.
6. Características del personal vinculado con las tecnologías y sus servicios, en particular su preparación, profesionalidad y experiencia.
7. Condiciones de las edificaciones, su ubicación, estructura, disposición de los locales y condiciones constructivas.

Al describir el sistema informático se emplean los esquemas, tablas, gráficos y otros medios auxiliares que se requieran; a fin de facilitar una mejor comprensión. Estos medios auxiliares pueden ser insertados, dentro de esta propia sección o al final del plan, como anexos a los cuales se hace obligada referencia.

La caracterización del sistema informático permite conocerlo con plenitud, facilita una mejor determinación de las necesidades de protección y evita pérdida de tiempo e imprecisiones. Su descripción en detalle posibilita al que la lea tener un conocimiento lo más exacto posible de este, aunque sea la primera vez que se enfrente a él, cuestión que es de gran utilidad cuando se producen cambios en el personal, lo que suele ocurrir con relativa frecuencia.

Un ejemplo de caracterización del sistema informático de la Empresa X podría ser:

"El sistema informático de la Empresa X está soportado en los medios informáticos que se describen en el Anexo No. 1, que incluyen servidores, computadoras de mesa y portátiles, gran parte de ellas conectadas en red.
En la Oficina Central existe una red local que abarca las áreas situadas en la planta baja y los pisos 4 y 5 del edificio de la calle Martí No. 610.
Para la gestión de la red se cuenta con 5 servidores que utilizan como sistema operativo Windows 2003 Enterprise y Linux Debian; en las estaciones de trabajo se emplea Windows XP y Linux Ubuntu.
Los servidores tienen la función de: controlador de dominio, aplicaciones, base de datos, correo electrónico y Proxy.
Los servicios implementados en la red son navegación Internet, correo electrónico y transferencia de ficheros. La navegación y el correo tienen alcance nacional o internacional en dependencia de lo aprobado para cada usuario a partir de sus necesidades.

Las aplicaciones y bases de datos en explotación son:

- *Sistema de Representación Geoespacial (SIRGE)*
- *Sistema Contable (CONTAB)*
- *Sistema de Control de Información Clasificada (SCIC)*
- *Sistema de Control de Componentes (Everest).*
- *Sistema de Control de Actualizaciones (WSUS)*

Además se utilizan los paquetes de Office y Open Office para la elaboración de informes y otros documentos, en las máquinas previstas para el trabajo interno.

El cableado de la red está soportado por cable UTP categoría 5, 100 Mbits, con topología estrella (Anexo 2), protegido con canaletas. Las estaciones de trabajo se agrupan por áreas y pisos a partir de conmutadores (switchs) capa 2.
Además se cuenta con un punto de acceso inalámbrico (Access Point) a la red de Internet en el salón de reuniones del quinto piso.
La conexión con el exterior se realiza con el uso de una línea arrendada de 1 Mbit conectada directamente al proveedor de servicios de Internet.

El intercambio de información tanto interna como externa se realiza básicamente a través del correo electrónico.

La información ordinaria de la Oficina Central se procesa en las estaciones de trabajo de la red y la información clasificada en máquinas independientes, ubicadas en la Dirección de la Empresa, en el Departamento de Cuadros y en el de Seguridad y Defensa. La información recibida desde las dependencias de la empresa y la que se envía al Organismo superior se tramita por medio del correo electrónico y de la Intranet. La información que se expone en la Intranet es en todos los casos de uso público.

El edificio de Martí 610 se encuentra cerca del litoral habanero, tiene buenas condiciones constructivas, adecuadas tanto para la protección como para la preservación de los equipos y la posibilidad de visibilidad de las pantallas desde el exterior es prácticamente nula.
El personal que opera los equipos posee los conocimientos y la preparación necesaria para su empleo y en la mayor parte de los casos tiene nivel medio o superior.”

3. Resultados del análisis de riesgos

Una vez definido el alcance del PSI y realizada una detallada descripción del sistema informático, corresponde finalizar esta primera parte con la formulación de las conclusiones obtenidas durante la determinación de las necesidades de protección, mediante la evaluación de los riesgos. Estas conclusiones incluyen:

a) Cuáles son los bienes informáticos más importantes para la gestión de la entidad y por lo tanto requieren de una atención especial desde el punto de vista de la protección; se especifican aquellos considerados de importancia crítica por el peso que tienen dentro del sistema;
b) qué amenazas pudieran tener un mayor impacto sobre la entidad en caso de materializarse sobre los bienes a proteger;
c) cuáles son las áreas con un mayor peso de riesgo y qué amenazas lo motivan.

Un ejemplo de los resultados del análisis de riesgos en la Empresa X podría ser:

Los bienes informáticos más importantes a proteger son:

- *La red de trabajo interno de la Oficina;*
- *El servidor de aplicaciones;*
- *Las bases de datos del sistema SIRGE (de importancia crítica);*
- *Las bases de datos de la intranet;*
- *El servicio de correo electrónico;*
- *El sistema contable CONTAB.*

Las amenazas más importantes a considerar de acuerdo con el impacto que pudieran tener sobre la empresa son:

- *El acceso no autorizado a la red, tanto producto de un ataque externo como interno.*
- *Pérdida de disponibilidad.*
- *La sustracción, alteración o pérdida de datos.*
- *Fuga de información clasificada.*
- *La introducción de programas malignos.*
- *El empleo inadecuado de las tecnologías y sus servicios.*
- *Las penetraciones del mar.*

Las áreas sometidas a un mayor peso/riesgo y las amenazas que lo motivan son:

- *El local de los servidores de la red (acceso no autorizado y pérdida de disponibilidad).*
- *El local de Economía (alteración o pérdida de datos, pérdida de disponibilidad y la introducción de programas malignos).*
- *El Departamento de Investigación y Desarrollo (alteración o pérdida de datos, pérdida de disponibilidad y la introducción de programas malignos).*
- *Las oficinas de la Dirección, del Departamento de Cuadros y del Departamento de Seguridad y Defensa (fuga de información clasificada).*
- *El almacén situado en la planta baja del edificio (penetraciones del mar).*

En la medida en que las conclusiones del análisis de riesgos sean más precisas se logra una visión más acertada de hacia dónde son dirigidos los mayores esfuerzos de seguridad y por supuesto los recursos disponibles para ello, y se logra que esta sea más rentable.

4. **Políticas de Seguridad Informática**

En esta sección se definen los aspectos que conforman la estrategia a seguir por la Entidad sobre la base de sus características, de conformidad con la política vigente en el país en esta materia y el sistema de seguridad diseñado.

Establecen las normas generales que cumple el personal que participa en el sistema informático y se derivan de los resultados obtenidos en el análisis de riesgos y de las definidas por las instancias superiores en las leyes, resoluciones, reglamentos, y otros documentos rectores.

Al definir las políticas de Seguridad Informática que son establecidas en la entidad se consideran los elementos expuestos en el punto No. 1.4.1 de la Primera Parte de esta Metodología.

Las políticas que se describan comprenden toda la organización, ya que es obligatorio su cumplimiento en las áreas que las requieran, razón por las que son lo suficientemente generales y flexibles para poder implementarse, en cada caso, mediante las medidas y procedimientos que demanden las características específicas de cada lugar.

A modo de ejemplo se muestran algunas de las políticas definidas en la Empresa X:

1. *Las propuestas de iniciativas encaminadas a mejorar el sistema de seguridad informática se aprueban por el Consejo de Dirección.*

2. *El acceso a las tecnologías de la entidad es expresamente aprobado en cada caso y el personal tiene que estar previamente preparado en los aspectos relativos a la seguridad informática.*

3. *Los usuarios de las tecnologías de la información y la comunicación responden por su protección y están en la obligación de informar cualquier incidente o violación que se produzca a su Jefe inmediato superior.*

4. *Todos los bienes informáticos son identificados y controlados físicamente hasta nivel de componentes.*

5. *Se establecen procedimientos que especifiquen quién y cómo se asignan y suspenden los derechos y privilegios de acceso a los sistemas de información.*
6. *Se prohíbe vincular cuentas de correo electrónico de la entidad a un servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través de este.*

7. *En caso de violación de la seguridad informática, se comunica al Jefe inmediato superior y a la Oficina de Seguridad para las Redes Informáticas y se crea una comisión encargada de analizar lo ocurrido y proponer la medida correspondiente.*

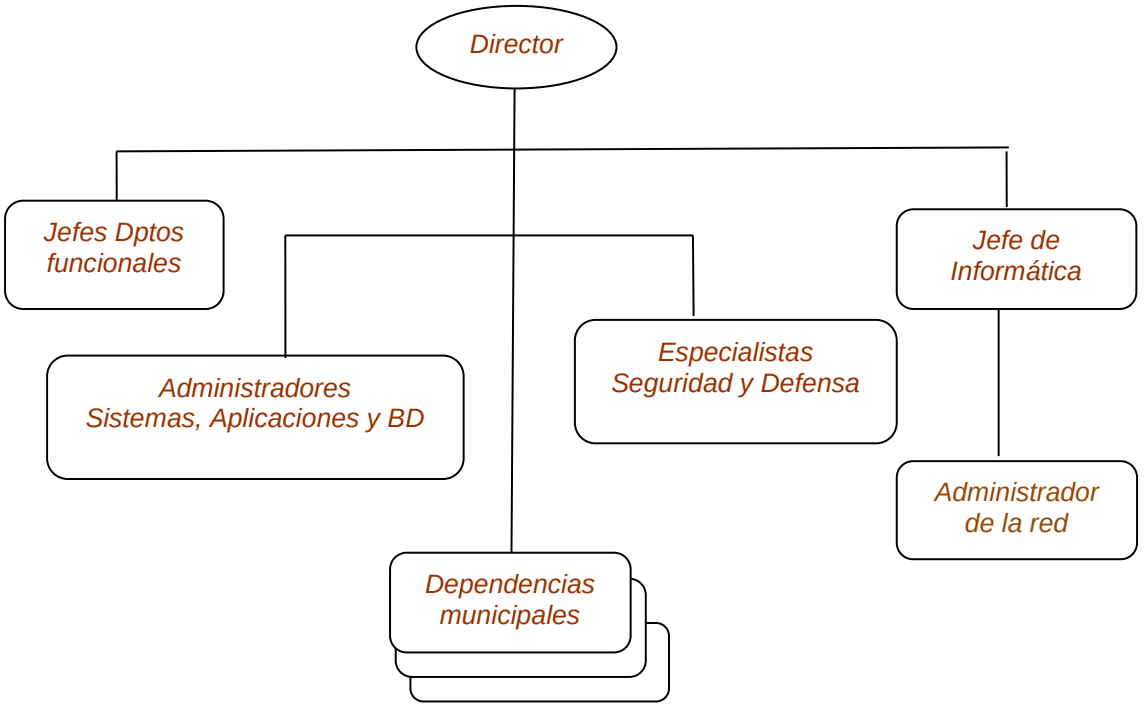
5. Responsabilidades

Se describe la estructura concebida en la Entidad para la gestión de la Seguridad Informática, se especifican las atribuciones, funciones y obligaciones de las distintas categorías de personal, que incluyen: directivos a los distintos niveles (jefe de la entidad, jefes de departamentos, áreas y grupos de trabajo o estructuras equivalentes); jefes y especialistas de informática; administradores de redes, sistemas y aplicaciones; especialistas de seguridad informática y de seguridad y protección y usuarios comunes de las tecnologías de Información.

Al especificar las atribuciones, funciones y obligaciones del personal en función de sus cargos, se tiene en cuenta lo establecido al respecto en el Reglamento de Seguridad para las TIC.

Un ejemplo de la estructura concebida para la gestión de la seguridad informática y de las funciones y obligaciones de los administradores de sistemas, aplicaciones y bases de datos en la Empresa X podría ser:

Estructura de gestión de la seguridad informática de la Empresa



Funciones y Obligaciones de los Administradores de Sistemas, Aplicaciones y Bases de Datos de la Empresa X.

a) *Informar a los usuarios de los controles de seguridad que hayan sido establecidos y verificar su utilización apropiada;*
b) *controlar el acceso a los sistemas, aplicaciones y bases de datos en correspondencia con la política establecida;*
c) *garantizar la ejecución de los procedimientos de salva de programas y datos, así como su conservación;*
d) *detectar posibles vulnerabilidades en los sistemas y aplicaciones bajo su responsabilidad y proponer acciones para su solución;*
e) *garantizar su mantenimiento y actualización y el registro de los sistemas y aplicaciones que lo requieran.*

Aplicaciones, Sistemas y Bases de Datos	***Administrador (poner nombres)***
Sistema de Representación Geoespacial (SIRGE)	*Jesús*
Sistema de Control de Componentes (Everest)	*Julio*
Sistema contable CONTAB	*Anaibis*
Sistema de control información clasificada (SCIC)	*Diana*
Sistema de Control de Actualizaciones (WSUS)	*Humberto*

6. Medidas y Procedimientos de Seguridad Informática

En este segmento del PSI se describe **cómo** se implementan, en las áreas a proteger, las políticas que han sido definidas para la entidad, en correspondencia con las necesidades de protección en cada una de ellas, de acuerdo con sus formas de ejecución, periodicidad, personal participante y medios**.** Se describen por separado los controles de seguridad implementados, en correspondencia con su naturaleza, se combinan el empleo de los recursos humanos y de los medios técnicos con las acciones que son realizadas.

Las medidas y procedimientos no deben confundirse con una declaración de intención o línea de deseos, por lo que con su descripción se especifican los controles implementados, no los que se quisieran implementar.

El PSI se sustenta sobre la base de los recursos disponibles y en dependencia de los niveles de seguridad alcanzados y de los aspectos que queden por cubrir se elabora un Programa de Desarrollo de la Seguridad Informática, que incluya las acciones a realizar por etapas para lograr niveles superiores (ver punto No. 2.1. de la Primera Parte).

Hay que concentrarse en las acciones que garantizan la instrumentación de las políticas definidas y su aplicación apropiada en cada área que lo requiere.

6.1. Clasificación y control de los bienes informáticos

Estas medidas y procedimientos persiguen identificar los bienes informáticos de acuerdo con su importancia, controlar y supervisar que sean utilizados en funciones propias del trabajo y garantizar su protección. En este apartado se incluyen las medidas y los procedimientos que se requieran para:

1. Precisar los métodos de supervisión y control que se utilicen, el personal encargado de ejecutarlos y los medios empleados para ello.
2. Establecer los mecanismos que se requieran para identificar y controlar los bienes informáticos y la conformación de su inventario permanentemente actualizado.
3. Precisar la persona encargada de cada bien informático y responsable por su protección.
4. Garantizar la autorización y el control sobre el movimiento de los bienes informáticos.

A modo de ejemplo de medidas y procedimientos de control de los medios informáticos se muestran los siguientes:

Medida:
La administradora del sistema CONTAB responde por la integridad de los medios destinados para la explotación de esta aplicación.

Procedimiento 1 *Control de medios informáticos.*

1. *Acceder la última semana de cada mes al Sistema de Control de Componentes (Everest) a través del servidor de la red y se aplica a los medios informáticos que forman parte del dominio de la red.*
2. *Comprobar cambios existentes desde el último control realizado.*
3. *Informar a la Dirección de la Empresa los resultados de la comprobación.*
4. *Generar un resumen de los resultados de cada control y conservarlo por un año.*
   Responsable: *Administrador de la red*
5. *Esclarecer en caso de existir diferencia, las causas y responsabilidades.*
   Responsable: *Director de la empresa*

6.2. Del Personal

Las medidas y procedimientos asociadas con el personal tienen como objetivo garantizar el cumplimiento de las funciones y responsabilidades de seguridad generales y específicas de las personas vinculadas con las TIC y sus servicios, así como la documentación de estas y aseguran:

1. La selección adecuada del personal previsto para ocupar cargos en la actividad informática o con acceso a sistemas críticos, a información de valor o a la supervisión y seguridad de los sistemas.
2. La obligación de la entidad en cuanto a la preparación del personal y la responsabilidad del trabajador hacia la Seguridad Informática, así como la inclusión de estos aspectos en los términos y condiciones del contrato de empleo.
3. La forma en que es autorizada por la dirección de la entidad la utilización de las tecnologías y sus servicios por parte de los usuarios que lo necesiten.
4. La obligación de los jefes a cada nivel en cuanto a garantizar la Seguridad Informática en su área de responsabilidad.
5. Las acciones a realizar en caso de empleo no autorizado de las tecnologías y sus servicios por parte de los usuarios.
6. La responsabilidad de los jefes a cada nivel en cuanto a la preparación de su personal y del conocimiento de sus deberes y derechos, incluyen la introducción en el contrato de trabajo de la constancia del compromiso de cada trabajador.
7. Los requerimientos de seguridad para la autorización del acceso a las tecnologías y servicios por parte de personal externo.
8. Las formas y medios mediante los cuales los usuarios informan acerca de cualquier incidente de seguridad, debilidad o amenaza.
9. Evitar la realización de acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros, así como la introducción, ejecución, distribución o conservación de programas para esos fines o información contraria al interés social, la moral y las buenas costumbres.

Los controles de seguridad en relación con el personal consideran no solo los requisitos a cumplir por los trabajadores durante el tiempo de vigencia de su contrato de empleo, sino también antes de ser contratado y con posterioridad al cese de su relación laboral.

Un ejemplo de procedimiento relacionado con el personal en la Empresa X podría ser:

Procedimiento 2 *Aprobación de acceso a las tecnologías y servicios por parte de personal externo.*

1. *Elaborar y presentar la solicitud de autorización de acceso a las TIC al Director de la Empresa, donde se incluya el nombre y apellidos de la persona que necesita el acceso y su número de carné de identidad; las razones que justifican este acceso, el acceso que se requiere y el tiempo que se requiera mantenerlo.*
   Responsable: *Jefe del área asociada con el acceso*

2. *Aprobar (denegar) la solicitud en caso que corresponda, y darlo a conocer por escrito al administrador de la red, al Jefe del área que realizó la solicitud y al Jefe del Departamento de Seguridad y Defensa, especifican el alcance del acceso y su tiempo de vigencia.*
   Responsable: *Director de la Empresa*
3. *Asignar (en caso de autorización de acceso), un identificador personal y único para el acceso a los sistemas y servicios determinados en la aprobación y definir en el servidor de la red los atributos en correspondencia con la autorización otorgada.*
   Responsable: *Administrador de la red*
4. *Imponer a la persona a que se otorga el acceso de sus obligaciones y atribuciones en relación con el empleo de las tecnologías y sus servicios.*
   Responsable*: Jefe del área que solicita el acceso*
5. *Solicitar al director la cancelación del acceso concedido e informar las razones de la solicitud.*
   Responsable: *Jefe del área que solicita el acceso*
6. *Cancelar la cuenta y los permisos de acceso una vez concluido el plazo previsto.*
   Responsable: *Administrador de la red.*

6.3. Seguridad Física y Ambiental

Las medidas y procedimientos de seguridad física y ambiental tienen como objetivo evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones, las tecnologías y la información de la organización.

Se aplican a los locales donde se encuentran las TIC y directamente a estas mismas tecnologías y a los soportes de información e incluyen: medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.

La protección física se alcanza con la creación de una o más barreras físicas alrededor de las áreas de procesamiento de la información. El uso de múltiples barreras brinda protección adicional, de modo que la falta de una barrera no significa que la seguridad se vea comprometida inmediatamente.
La protección del equipamiento (incluyen aquel utilizado fuera de la entidad) es necesaria para reducir el riesgo de accesos no autorizados a la información y para protegerlo contra pérdidas o daños. Se pueden requerir controles especiales para proteger contra amenazas físicas, y para preservar los equipos, tales como la garantía del suministro eléctrico y la infraestructura adecuada del cableado.

La seguridad ambiental incluye la aplicación de medios contra daños que puedan ser ocasionados por incendios, inundaciones, terremotos, explosiones, perturbación del orden, y otras formas de desastre natural o artificial.

Las medidas y procedimientos de seguridad física y ambiental van dirigidas a:

1. La protección de las tecnologías contra la sustracción o alteración, e incluyen sus componentes y la información que contienen.
2. Impedir su empleo para cometer acciones malintencionadas o delictivas.
3. Disminuir el impacto producido por fuego, inundación, explosión, perturbación del orden y otras formas de desastre natural o artificial.
4. La protección contra fallas de alimentación u otras anomalías eléctricas.
5. La protección de los cables que transporten datos o apoyen los servicios contra la intercepción o el daño.
6. Garantizar que el equipamiento reciba un mantenimiento adecuado en correspondencia con las especificaciones del fabricante.
7. El control del movimiento de las tecnologías.
8. La preservación de la información del equipamiento que cause baja o se destine a otras funciones.

Corresponde a esta parte del PSI la determinación de los locales considerados como áreas o zonas controladas, en correspondencia con la caracterización del sistema informático realizado y los resultados del análisis de riesgos y que por lo tanto tienen requerimientos específicos de seguridad, en base a lo cual se declaran áreas **limitadas, restringidas o estratégicas** y se describen las medidas que se aplican en cada una de ellas, por ejemplo: restricciones para limitar el acceso a los locales, procedimientos para el empleo de cierres de seguridad y dispositivos técnicos de detección de intrusos y otros.

Al referir las medidas y procedimientos que se establecen para lograr una seguridad física y ambiental adecuada a las necesidades de las TIC, no es necesario describir las condiciones constructivas de los inmuebles, pues ya eso ha sido realizado durante la caracterización del sistema informático y expuesto en el punto 2 de la estructura del PSI.

Un ejemplo de la clasificación y medidas específicas en las áreas controladas en la Empresa X es la siguiente:

Área controlada	***Categoría***	***Medidas específicas***
Dirección, Cuadros, Seguridad y Defensa	*Limitada*	*Acceso físico limitado; cierres seguros en puertas y ventanas; alarma contra intrusos.*
Economía	*Limitada*	*Acceso físico limitado; control de soportes removibles; alarma contra intrusos; separación de funciones; protección de las copias de programas y datos.*
Servidores de la red	*Limitada*	*Acceso solo a administradores; cierre magnético en la puerta de acceso y alarma contra intrusos: redundancia de HW, SW, climatización y datos.*
Investigación y Desarrollo	*Limitada*	*Acceso físico limitado; cierres seguros en puertas y ventanas; alarma contra intrusos; redundancia de datos.*

Se describen en detalle las medidas específicas de la tercera columna de la tabla anterior: a quien se autoriza el acceso, tipo de alarma, en que consiste el cierre seguro, como se controlan los soportes removibles, que funciones están separadas en usuarios diferentes, como se logra la redundancia y la protección de la información de respaldo y otros.

Obsérvese que las áreas declaradas como controladas coinciden con las que se determinó en el análisis de riesgos que estaban sometidas a un mayor peso de riesgo (ver punto 3 de la estructura del PSI, Resultados del análisis de riesgos).

En el próximo ejemplo se muestra una medida con el procedimiento correspondiente para el control del movimiento de las tecnologías:

Medida:

La entrada, salida y traslado de las TIC en la Empresa X se realiza con autorización del Director en correspondencia con el Procedimiento 3, dejan constancia de ello en el Registro1, movimiento de TIC.

Procedimiento 3 Movimiento de las TIC

1. *Solicitar autorización por escrito al Director de la Empresa X para el movimiento de las tecnologías que lo requieran, fundamentan en qué consiste el movimiento, los motivos y si es temporal el tiempo requerido.*
   Responsable: *Jefe del área a que pertenece el medio a trasladar*

2. *Autorizar si es procedente el movimiento de las tecnologías y darlo a conocer por escrito al Jefe del área que realizó la solicitud, al Jefe del área de Contabilidad y al Jefe del Departamento de Seguridad y Defensa, especifican el tiempo de vigencia de la autorización.*
   Responsable: *Director de la Empresa X*
3. *Registrar en el sistema CONTAB el movimiento del medio básico autorizado a trasladar.*
   Responsable*: Jefe del área de Contabilidad.*
4. *Revisar antes de su salida (entrada) de la entidad las tecnologías autorizadas a trasladar, precisan la existencia y estado de sus partes y componentes, si contienen información y de qué tipo, así como lo relacionado con el control antivirus.*
   Responsable: *Jefe del área a que pertenece el medio a trasladar*
5. *Consignar el movimiento en el Registro 1, especifican la fecha en que se produce, los datos del equipo objeto del movimiento, de qué lugar se extrae o proviene y a qué lugar se lleva y motivo por el que se realiza el movimiento (evento, exposición, reparación y otros.).*
   Responsable: *Jefe del área a que pertenece el medio a trasladar*
6. *Controlar el cumplimiento de las autorizaciones sobre el movimiento de las tecnologías y su registro adecuado.*
   Responsable: *Jefe del Departamento de Seguridad y Defensa*

6.4. Seguridad de Operaciones

Las medidas y procedimientos de Seguridad de Operaciones están dirigidas a lograr una eficiente gestión de la seguridad y garantizan el cumplimiento de las regulaciones vigentes en el país, así como las establecidas por la propia entidad.

La gestión del sistema de seguridad implica el control de las acciones que se realizan dentro del sistema informático y su garantía de que se ajustan a las políticas de seguridad establecidas para el empleo de las tecnologías y sus servicios, y para ello las medidas y procedimientos de seguridad de operaciones consideran, entre otros, los aspectos siguientes:

1. La aplicación del principio de separación de funciones evita que se asignen a una misma persona tareas que en su conjunto pueden propiciar la modificación no autorizada de datos o el mal uso de los sistemas.
2. La aprobación para la introducción en la entidad de nuevos sistemas informáticos, actualizaciones y nuevas versiones, previa verificación de su correspondencia con

el sistema de seguridad establecido y el cumplimiento de los criterios de seguridad apropiados.

3. El control por el personal autorizado de las acciones necesarias para cubrir las brechas de seguridad y la corrección de los errores de los sistemas, su documentación y reporte a quienes corresponda.

En esta parte del PSI se incluye la ejecución de los procedimientos de revisión mediante los métodos de medición que posibiliten detectar errores de proceso, identificar fallos de seguridad de forma rápida y determinar las acciones a realizar para lograr el ciclo de mejora continúa. Se utilizan para ello los indicadores seleccionados sobre la base de los criterios respecto a qué aspectos se controlan y miden para lograr el cumplimiento de los objetivos planteados en el SGSI implementado en la entidad. Existen diversos métodos de medición y hay disponibles diferentes procedimientos y herramientas que facilitan su implementación en cualquier entidad (ver punto 3 de la Primera Parte, Proceso de Verificación del SGSI).
Se incluyen además las medidas y procedimientos implementados para el registro y análisis de las trazas de auditoría generadas por los sistemas operativos y servicios de redes, y por los sistemas instalados según lo reglamentado, con el fin de monitorear las acciones que se realicen (acceso a ficheros, dispositivos, empleo de los servicios y otros), y detectar indicios de hechos relevantes a los efectos de la seguridad que puedan afectar la estabilidad o el funcionamiento del sistema informático.

En caso de empleo de software especializado que permita la detección de posibles errores de configuración u otras vulnerabilidades, así como su corrección, se describen los procedimientos requeridos.

Se refieren además las medidas que garanticen la integridad de los mecanismos y registros de auditoría limitan su acceso solo a las personas autorizadas para ello.

A modo de ejemplo de procedimiento de las acciones necesarias para cubrir las brechas de seguridad y la corrección de los errores en la Empresa X se muestra el siguiente:

***Procedimiento 4* Corrección de errores y brechas de seguridad.**

1. *Instalar y configurar las aplicaciones Wsus, destinada para distribuir parches de seguridad de Microsoft para la eliminación de vulnerabilidades conocidas cuando su solución sea publicada por el fabricante y LANguard y Nmap, para detectar brechas de seguridad, puertos abiertos y otras vulnerabilidades similares.*

Responsable: *Administrador de la red*

2. *Ejecutar las aplicaciones LANguard y Nmap una vez al mes y controlar cada lunes la ejecución de Wsus.*

   Responsable: *Administrador de la red*

3. *Informar los resultados de las acciones de corrección de errores y brechas de seguridad al Jefe del Departamento de Informática cada vez que se realicen y preservar los registros en los soportes habilitados al efecto por un tiempo no menor de un año.*

   Responsable: *Administrador de la red*

4. *Analizar los resultados de las acciones de corrección de errores y brechas de seguridad y su correspondencia con lo previsto en el Sistema de Seguridad Informática de la Empresa y, en caso de detectarse nuevas vulnerabilidades, proponer las acciones necesarias para su evaluación y determinación de las modificaciones requeridas para su eliminación.*

   Responsable: *Jefe del Departamento de Informática*

5. *Actualizar los cambios en el PSI.*

   Responsable: *Jefe del Departamento de Informática*

6.5. Identificación, Autenticación y Control de Acceso

Las medidas y procedimientos de identificación, autenticación y control de acceso responden a las políticas que previamente fueron definidas en la entidad sobre estos aspectos, y tienen como objetivo gestionar el acceso a la información de forma segura, garantizan el acceso de usuarios autorizados e impiden el acceso no autorizado a los sistemas de información. Los accesos a la información y a las instalaciones de procesamiento de la información son controlados sobre la base de requisitos de seguridad. Los controles consideran:

a) Las políticas para la autorización y distribución de la información.
b) La consistencia entre los controles de acceso y las políticas de clasificación de la información.
c) La legislación vigente y las obligaciones contractuales con respecto a la protección del acceso a los datos o servicios.
d) El establecimiento de perfiles estándar de acceso de usuarios para roles comunes.
e) La gestión de derechos de acceso en un ambiente distribuido y de redes, que reconozca todos los tipos de conexión posibles.
f) La separación de roles de control de acceso, por ejemplo, solicitud de acceso, autorización de acceso y administración de acceso.
g) Los requisitos para autorizaciones formales de solicitudes de acceso.

h) La cancelación de derechos de acceso.

Esos controles cubren todas las etapas del ciclo de vida del acceso del usuario, desde el registro inicial de nuevos usuarios hasta la cancelación final del registro de usuarios que no requieren más acceso a los sistemas de información y a los servicios.

Identificación de usuarios

Los procedimientos de identificación de usuarios garantizan:

a) la utilización de un identificador único (ID) para cada usuario para permitir que queden vinculados y sean responsables de sus acciones;
b) la verificación de que el usuario tenga autorización para el uso del servicio o el sistema de información;
c) la verificación de que el nivel de acceso otorgado se corresponda con la necesidad de uso y que es consistente con la política de seguridad, por ejemplo que no compromete la segregación de tareas;
d) que los usuarios firmen declaraciones indica que ellos comprenden y asumen las condiciones de acceso;
e) mantener un registro impreso de todas las personas a las que se les otorga acceso;
f) eliminar inmediatamente o bloquear los derechos de acceso de los usuarios que hayan cambiado roles o tareas o dejado la organización; y
g) realizar periódicamente una verificación para eliminar o bloquear las cuentas e identificadores de usuarios (ID´s) redundantes.

Se explica el método empleado para la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes, y se especifica:

1. Cómo se asignan los identificadores de usuarios.
2. Si existe una estructura estándar para la conformación de los identificadores de usuarios.
3. Quién asigna los identificadores de usuarios.
4. Cómo se eliminan los identificadores de usuarios una vez que concluya la necesidad de su uso y cómo se garantiza que estos no sean utilizados nuevamente.
5. El proceso de revisión de utilización y vigencia de los identificadores de usuarios asignados.

Autenticación de usuarios

Se explica el método de autenticación empleado para comprobar la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes.

Cuando se utilice algún dispositivo específico de autenticación, se describe su forma de empleo. En el caso de empleo de autenticación simple por medio de contraseñas se especifica:

1. Cómo son establecidas las contraseñas.
2. Tipos de contraseñas utilizadas (configuración de arranque, protector de pantalla, aplicaciones).
3. Estructura y periodicidad de cambio que se establezca para garantizar la fortaleza de las contraseñas utilizadas en los sistemas, servicios y aplicaciones, en correspondencia con el peso de riesgo estimado para estos.
4. Causas que motivan el cambio de contraseñas antes de que concluya el plazo establecido.

La estructura y periodicidad de cambio de las contraseñas de acceso son seleccionadas en correspondencia con la importancia de los bienes cuyo acceso se protege y los riesgos a que están sometidos, así como la existencia de otros tipos de controles complementarios que contribuyan a su protección, por lo que no necesariamente son iguales en todos los casos. Por ejemplo, para un sistema que no está catalogado como de importancia crítica para la entidad y que además está ubicado en un área a la que no acceden muchas personas, tal vez una contraseña de pocos caracteres que se modifique en intervalos largos sería suficiente, por el contrario un sistema de importancia crítica para la entidad cuenta con contraseñas de mayor fortaleza, se obliga a su cambio con mayor frecuencia.

En una red, con este objetivo podrían crearse grupos con necesidades de seguridad comunes, a los cuales se les impondrían requerimientos diferenciados en cuanto a la estructura y cambio de las contraseñas de acceso.

La instauración de contraseñas se controla a través de un proceso formal de gestión. El proceso incluye los requisitos siguientes:

a) exigir a los usuarios que firmen una declaración de que se comprometen a mantener confidencialidad sobre las contraseñas personales; esta declaración

firmada se incluye dentro de los términos de empleo como parte de sus responsabilidades hacia la Seguridad Informática (ver punto 6.2 “Del Personal”);

b) establecer procedimientos para verificar la identidad del usuario antes de la utilización de cualquier contraseña;
c) cuando se asigne inicialmente una contraseña temporal, los usuarios son forzados a cambiarla inmediatamente después del primer acceso;
d) las contraseñas temporales son proporcionadas a los usuarios de un modo seguro y se evita el uso de mensajes de correo electrónico de terceras partes o no protegidos (en texto claro);
e) las contraseñas por defecto de los vendedores se cambian inmediatamente luego de la instalación del software o sistemas; y
f) las contraseñas son únicas para cada persona y no son descifrables.

Las contraseñas son un medio común de verificación de la identidad del usuario antes de acceder a los sistemas de información o a los servicios, de acuerdo con la autorización que tenga el usuario, pero es un método que puede ser violado con relativa facilidad. En los casos que se requiera una mayor seguridad, se consideran otras tecnologías disponibles para la identificación y autenticación del usuario, tales como biometría, por ejemplo, verificación de huella digital, verificación de firma, y uso de medios físicos de autenticación como tarjetas inteligentes.

Se exige a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas. Todos los usuarios son advertidos en cuanto a:

a) mantener confidencialidad sobre la contraseña;
b) evitar mantener un registro de contraseñas en texto claro en cualquier medio (por ejemplo, papel, archivo de software o dispositivo de mano);
c) cambiar las contraseñas cuando haya una indicación de riesgo en el sistema o en la contraseña;
d) seleccionar contraseñas de calidad con suficiente longitud mínima que sean:
    1. Fáciles de recordar.
    2. No se basen en algo que alguien pueda adivinar fácilmente o usen información relacionada con la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento, etc.
    3. No vulnerables a ataques tipo diccionario (es decir, que no consistan en palabras incluidas en diccionarios).
    4. Libres de caracteres idénticos sucesivos ya sean numéricos o alfabéticos.

e) Cambiar las contraseñas a intervalos regulares o basados en el número de accesos (las contraseñas de cuentas privilegiadas son cambiadas más frecuentemente que las contraseñas normales), y evitar la reutilización o reciclaje de contraseñas;
f) cambiar las contraseñas temporales en la primera conexión;
g) no incluir contraseñas en ningún proceso automatizado de conexión;
h) no compartir las contraseñas de usuario individuales; y
i) no utilizar la misma contraseña para propósitos de trabajo y particulares.

Control de acceso a los bienes informáticos

Se describen las medidas y procedimientos que aseguran el acceso autorizado a los bienes informáticos que requieren la imposición de restricciones a su empleo, se especifica:

1. A qué bienes informáticos se le implementan medidas de control de acceso.
2. Métodos de control de acceso utilizados.
3. Quién otorga los derechos y privilegios de acceso.
4. A quién se otorgan los derechos y privilegios de acceso.
5. Cómo se otorgan y suspenden los derechos y privilegios de acceso.

El control de acceso a los bienes informáticos está basado en una política de “mínimo privilegio”, en el sentido de otorgar a cada usuario solo los derechos y privilegios que requiera para el cumplimiento de las funciones que tenga asignadas.

La asignación de derechos y privilegios es controlada a través de procedimientos formales de autorización que determinan el perfil de cada usuario. Se consideran los elementos siguientes:

a) asociar el derecho de acceso con cada componente, por ejemplo sistema operativo, sistema de gestión de base de datos y de cada aplicación, identifican los usuarios a los que es necesario asignar tales privilegios;
b) los privilegios son asignados sobre la base de necesidad de uso y consideran recurso por recurso;
c) se implementa un proceso de autorización y se mantiene un registro de todos los privilegios asignados; los privilegios no se otorgan hasta que el procedimiento de autorización concluya.

Hay que tener en cuenta que el uso inapropiado de los privilegios de administración puede ser un factor importante de surgimiento de fallas o brechas de seguridad (cualquier característica o recurso de un sistema informático que habilite al usuario a hacer caso omiso de los controles de este o de la aplicación).

La dirección de la entidad instrumenta la revisión de los derechos de acceso de los usuarios a intervalos regulares para mantener un control efectivo sobre el acceso a los datos y servicios informáticos, utilizan un proceso formal que considere los siguientes aspectos:

a) los derechos de acceso de usuarios son revisados después de cualquier cambio, tal como el traslado de un cargo a otro dentro de esta organización, o el cese de las relaciones laborales; y
b) verificar que con la asignación de derechos no se obtienen privilegios no autorizados.

Como parte del control de acceso a los bienes informáticos se incluyen las medidas y procedimientos establecidos, con el fin de evitar la modificación no autorizada, destrucción y pérdida de los ficheros y datos, así como para impedir que sean accedidos públicamente, se especifican:

1. Medidas de seguridad implementadas a nivel de sistemas operativos, aplicación o ambos, para restringir y controlar el acceso a las bases de datos.
2. Medidas para garantizar la integridad del software y la configuración de los medios técnicos.
3. Empleo de medios criptográficos para la protección de ficheros y datos.

Ejemplo de procedimiento en la Empresa X

<u>Procedimiento 5</u> Aprobación y cancelación de acceso a las TIC

1. *Elaborar y presentar la solicitud de autorización (cancelación) de acceso a las TIC al Director de la Empresa, donde se incluya el nombre y apellidos del trabajador que necesita el acceso; las razones que justifican este acceso y los activos a que solicita acceder. De ser una necesidad temporal especifica el tiempo que se requiera mantenerlo. En el caso de retiro del acceso presenta breve informe que refiere los motivos de la propuesta y si es definitiva o temporal.*
   Responsable: *Jefe del área a que pertenece el trabajador*

2. *Aprobar (denegar) la solicitud en caso que corresponda, y darlo a conocer por escrito al administrador de la red y al Jefe del área que realiza la solicitud, especifica el alcance del acceso.*
   ***Responsable:** Director de la Empresa*
3. *Preparar al trabajador en el uso adecuado de las TIC y en sus obligaciones como usuario de estas y firma por el trabajador del compromiso de empleo de estas. El documento original se entrega al administrador de la red y la copia se incluye en el contrato de trabajo.*
   ***Responsable:** Jefe del área a que pertenece el trabajador*
4. *Asignar (en caso de autorización de acceso), un identificador personal y único para el acceso a los sistemas y servicios determinados en la aprobación y definir en el servidor los atributos en correspondencia con la autorización otorgada.*
   ***Responsable:** Administrador de la red*
5. *Otorgar al usuario una contraseña temporal para ser utilizada en su primera conexión, se obliga a cambiarla una vez que acceda al sistema o servicio asignado.*
   ***Responsable:** Administrador de la red*
6. *Configurar en el servidor los atributos que se determinen o se agregan en correspondencia con la autorización otorgada.*
   ***Responsable:** Administrador de la red*
7. *Cancelar, en caso de revocación de acceso, la cuenta y los permisos de acceso otorgados.*
   ***Responsable:** Administrador de la red*
8. *Conservar las autorizaciones de acceso a las TIC en el área de informática por un período no menor de 1 año.*
   ***Responsable:** Jefe del Departamento de Informática*
9. *Realizar un control trimestral de este procedimiento e informar de sus resultados al Director de la Empresa.*
   ***Responsable:** Jefe del Departamento de Organización y Supervisión*

6.6. Seguridad ante programas malignos

Se establecen las medidas y procedimientos que se requieran para la protección contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para evitar su generalización, se especifican los programas antivirus utilizados y su régimen de instalación y actualización.

La protección contra códigos maliciosos se basa en el empleo de medidas de prevención, detección y recuperación, en la necesidad de la seguridad, y en controles apropiados de acceso al sistema. Las siguientes pautas son consideradas:

1. Establecimiento de políticas que instituyan la prohibición del uso de software no autorizado y la protección contra los riesgos asociados a la obtención de archivos y software por redes externas o cualquier otro medio, indican las medidas protectoras a adoptar.
2. Revisiones regulares del contenido de datos y software que soportan los procesos de gestión de la entidad y de la presencia de archivos no aprobados o modificaciones no autorizadas.
3. La instalación y actualización regular de programas antivirus que exploren las computadoras y los soportes de forma rutinaria o como un control preventivo para la detección y eliminación de código malicioso; las verificaciones incluyen:
   a) Comprobación de archivos en medios electrónicos u ópticos, y archivos recibidos a través de redes, para verificar la existencia de código malicioso, antes de su uso;
   b) comprobación de todo archivo adjunto a un correo electrónico o de cualquier descarga antes de su uso; realizar esta comprobación en distintos lugares, por ejemplo, en los servidores de correo, en las computadoras terminales o a la entrada de la red de la organización;
   c) comprobación de páginas Web para saber si existe en ellas código malicioso.

4. La definición de procedimientos y responsabilidades de gestión para la protección de los sistemas contra código malicioso, la capacitación para su uso, la información de los ataques de los virus y las acciones de recuperación.
5. La implementación de medidas para la recuperación ante ataques de código malicioso, incluyen los datos y software necesarios de respaldo y las disposiciones para la recuperación.
6. La implementación de procedimientos para obtener información sobre nuevos códigos maliciosos a través de listas de correo y comprobación de los sitios Web que brindan esa información.
7. La implementación de procedimientos para verificar la información relativa al software malicioso y asegurarse que es real; los encargados de esta actividad pueden diferenciar los códigos maliciosos reales de los falsos avisos de código malicioso, para lo que usan fuentes calificadas; se advierte al personal sobre el problema de los falsos avisos de código malicioso y qué hacer en caso de recibirlos.

Ejemplo de procedimiento en la Empresa X

***Procedimiento 6* Descontaminación de programas malignos**

1. *Al detectar en una estación de trabajo indicios de contaminación detener la actividad que se realiza, desconectarla de la red e informar al Jefe inmediato y al Administrador de la red.*
   ***Responsable:** Usuario de la estación de trabajo*
2. *Identificar de qué tipo de programa maligno se trata.*
3. *Verificar que en el medio contaminado se ejecuta una versión actualizada del programa antivirus instalado y de no cumplirse, proceder a la actualización del programa antivirus y llevar a cabo la descontaminación. De ser exitosa la descontaminación, poner en operación el medio afectado.*
4. *Revisar los soportes y el resto de las tecnologías que pudieran haber sido afectadas.*
5. *Investigar las causas de aparición del código malicioso.*
6. *Realizar las anotaciones pertinentes en el Registro de Incidencias (Registro No. 3).*
7. *Reportar el incidente a su instancia superior y a la OSRI.*
8. *Si es un programa maligno desconocido, proceder al aislamiento del fichero contaminado y remitirlo a la empresa Segurmática.*
   ***Responsable:** Administrador de la red*

6.7. Respaldo de la Información

Las medidas y procedimiento de respaldo que se implementen garantizan mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información frente a cualquier eventualidad.

Para alcanzar un nivel de respaldo adecuado se hacen las copias de seguridad de la información y del software que se determinen en cada caso y se comprueban regularmente.

Se dispone de procedimientos de respaldo para asegurar que toda la información esencial y el software puedan recuperarse tras un desastre o fallo, considerar para ello los elementos siguientes:

a) definir el nivel necesario de información de respaldo;
b) realizar copias seguras y completas de la información, y establecer los procedimientos de restauración;

c) determinar el grado (completo o parcial) y la frecuencia de los respaldos en correspondencia con los requisitos de la entidad, los requisitos de seguridad de la información implicada, y la importancia de la información que permita la operación continúa de la organización;
d) precisar las copias que son almacenadas en un área apartada del lugar habitual de procesamiento de la información que se preserva, a una suficiente distancia para la salvaguarda de cualquier daño producto de un desastre en el sitio principal;
e) establecer un nivel apropiado de protección ambiental y físico (ver punto 6.3. “Seguridad Física y Ambiental”) de la información de respaldo, consistente con las normas aplicadas en el sitio principal; los controles aplicados a los soportes en el sitio principal se extienden para cubrir el sitio de respaldo;
f) probar regularmente los soportes de respaldo para verificar que puede confiarse en ellos para el uso cuando sean necesarios;
g) comprobar regularmente los procedimientos de restauración para asegurar que son eficaces y que pueden ser utilizados dentro del tiempo asignado en los procedimientos de recuperación; y
h) proteger los respaldos por medio del cifrado en los casos que se requiera.

Para los sistemas críticos, las disposiciones de respaldo cubren la información y datos para recuperar el sistema completo en caso de un desastre.

Los procedimientos de respaldo, cuando sea posible, se automatizan para facilitar el respaldo y los procesos de restauración. Tales soluciones automatizadas se prueban suficientemente, antes de la puesta en práctica y en intervalos regulares.

Ejemplo de un procedimiento de respaldo en la Empresa X

***Procedimiento 7* Respaldo de Aplicaciones.**

1. *Realizar diariamente la salva de:*
    a) *Sistema Contable (CONTAB).*
    b) *Sistema de Control de Información Clasificada (SCIC).*
    c) *Sistema de Control de componentes (Everest).*
    d) *Sistema de Control de Actualizaciones (WSUS).*
    e) *Sistema de Representación Geoespacial (SIRGE).*

    Al finalizar la jornada de trabajo en discos compactos en dos versiones. Una copia es guardada en el local del administrador de la red y la otra en la oficina de la secretaria del director.

Responsable: *Administradores de sistemas*

2. *Verificar la integridad de la salva.*
   Responsable: *Administradores de sistemas*
3. *Consignar en el registro de salvas de aplicaciones (Registro 4) las acciones de respaldo realizadas*
   Responsable: *Administradores de sistemas*
4. *Realizar un control trimestral (incluyen revisión del registro), del cumplimiento de este procedimiento.*
   Responsable: *Jefe Departamento de Organización y Supervisión*

6.8. Seguridad en Redes

En esta parte del plan se incluyen las acciones a realizar para garantizar la seguridad de las redes y sus servicios, mediante la habilitación de las opciones de seguridad con que cuentan los sistemas operativos y de otras iniciativas dirigidas a lograr la seguridad de los servidores y terminales, el acceso a la información solamente por el personal autorizado y los elementos que permitan el monitoreo y auditoría de los principales eventos.
Se describe la configuración de los componentes de seguridad de las redes y servicios implementados y la instalación de los medios técnicos destinados a establecer una barrera de protección entre las tecnologías de la entidad y las redes externas. Para lo cual se tiene en cuenta:

1. Barreras de protección y su arquitectura.
2. Empleo de Cortafuegos, Sistemas Proxy y otros.
3. Filtrado de paquetes.
4. Herramientas de administración y monitoreo.
5. Habilitación de trazas y subsistemas de auditoría.
6. Establecimiento de alarmas del sistema.
7. Dispositivos de identificación y autenticación de usuarios.
8. Software especial de seguridad.
9. Medios técnicos de prevención y detección de intrusos (IPS/IDS).

Se especifican los procedimientos requeridos para el cumplimiento de las obligaciones de los administradores de redes en relación con la seguridad, en particular los relacionados con:

1. La aplicación de los mecanismos que implementan las políticas de seguridad aprobadas.
2. El análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red.

3. El análisis del empleo de los servicios de red implementados.
4. Las acciones de respuesta en caso de la ocurrencia de incidentes o actividades nocivas.

Se incluyen los procedimientos instrumentados para la verificación de la seguridad de las redes y la detección de vulnerabilidades.

Ejemplo de un procedimiento de auditoría de eventos del sistema operativo en la Empresa X

***Procedimiento 8* Auditoría de eventos del sistema operativo.**

1. *Realizar diariamente la revisión y análisis de los registros de los eventos generados por el sistema operativo de la red.*
2. *Investigar las causas de cualquier anomalía detectada y determinar si se está en presencia de un incidente de seguridad, actúa según lo establecido para esos casos.*
3. *Emplear, cuando se requiera, el software SAWMILL para la revisión de las trazas de auditoría.*
4. *Anotar las acciones realizadas y sus resultados en el registro de auditorías de eventos del S.O. (Registro 5).*
5. *Mantener la disponibilidad y actualización de las herramientas que garantizan la auditoría de los eventos del sistema operativo.*
   ***Responsable:** Administrador de la red*
6. *Realizar una verificación trimestral del cumplimiento de este procedimiento.*
   ***Responsable:** Jefe Departamento de Informática*

6.9. Gestión de Incidentes de Seguridad

Se describen las medidas y procedimientos de detección, neutralización y recuperación ante cualquier eventualidad que pueda paralizar total o parcialmente la actividad informática o degraden su funcionamiento, minimizan el impacto negativo de éstas sobre la entidad.
Los incidentes de seguridad incluyen entre otros:

1. Acceso (intentos de acceso) no autorizado a un sistema o sus datos.
2. Interrupción no deseada o negación de servicio.
3. Uso no autorizado de un sistema para el procesamiento o almacenamiento de información.
4. Suplantación de identidad.

5. Cambios a las características del equipamiento, las aplicaciones o datos del sistema sin el conocimiento o consentimiento del responsable de dicho sistema.

Al producirse los incidentes es fundamental que existan los mecanismos para:

1. Detectar e identificar eficazmente el incidente.
2. Crear estrategias de mitigación y respuesta.
3. Establecer canales confiables de comunicación.
4. Proporcionar alertas tempranas a quien lo requiera.
5. Ofrecer una respuesta coordinada a los incidentes.

A partir de los resultados obtenidos en el análisis de riesgos, se determinan las acciones a realizar para neutralizar aquellas amenazas que tengan mayor probabilidad de ocurrencia en caso de materializarse, así como para la recuperación de los procesos, servicios o sistemas afectados, precisan en cada caso:

1. Qué acciones se realizan.
2. Quién las realiza.
3. Cómo se realizan.
4. De qué recursos se dispone.

Los procedimientos para la gestión de incidentes especifican los pasos a seguir para garantizar:

1. La correcta evaluación de lo ocurrido.
2. A quién, cómo y cuándo se reportan.
3. Los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial.

Se habilita un registro donde se consignan los incidentes que se produzcan en la entidad, que es conservado por un período no menor de cinco (5) años y es utilizado como criterio de medición para la gestión del sistema de seguridad informática.

Ejemplo de un procedimiento de gestión de incidentes en la Empresa X

<u>Procedimiento 9</u> Interrupción en las comunicaciones

1. Informar a la Dirección de la Empresa la situación que se ha presentado.

2. *Identificar si la interrupción es causada por factores externos o internos.*

3. *Reportar la interrupción al proveedor del servicio si el problema radica en la línea de comunicación.*

4. *Restablecer la operación y establecer las causas de la interrupción y determinar posibles acciones para evitar su reiteración una vez solucionado el problema.*

5. *Anotar las acciones realizadas y sus resultados en el registro de incidencias. (Registro 6).*

6. *Reportar el incidente a la OSRI.*
   Responsable: *Administrador de la red*

7. Anexos del Plan de Seguridad Informática

7.1 Listado nominal de Usuarios con acceso a los servicios de red

Se habilita un listado de usuarios autorizados por cada servicio, especifican nombre, apellidos y cargo que ocupa en la entidad, así como los servicios para los que está autorizado.

7.2 Registros

Se definen los documentos de registro que se determinen a partir de los eventos y procedimientos que demanden dejar constancia, ya sea por requerimientos legales y de supervisión, con fines de análisis para elaborar tendencias o simplemente para el control de las actividades que se realizan, en correspondencia con las necesidades del SGSI implementado.

7.3 Control de Cambios

Se dispone de un modelo donde se registren aquellos cambios que motivan variaciones en el PSI y que por su magnitud no ameritan editar el plan en su totalidad nuevamente. Se incluyen los cambios que se realicen, la fecha, la parte del plan que se modifica, el nombre de la persona que autoriza la modificación y el de la persona que la realiza.