# GUÍA DE ESTUDIO DE SEGURIDAD INFORMÁTICA

1- ¿Qué es la Seguridad Informática?

R/ El conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas, detectar y responder acciones que pongan en riesgo la confidencialidad y disponibilidad de la información que se procese intercambie reproduzca y conserve a través de las tecnologías de información.

2- ¿Cómo se establecerá; La política en la entidad?

R/ Acorde a las regulaciones que rijan sobre la seguridad de la Información que se procese intercambia, reproduzca o conserve a través de las tecnologías de información, determinará los tipos de información y recursos para su protección y creará y establecerá los mecanismos de control para garantizar el cumplimiento de las regulaciones previstas en este Reglamento.

3- ¿Qué se hará para garantizar la Política Informática en cada entidad?

R/
Un análisis de la gestión informática que debe abarcar: organización, flujo de la información, tecnología de información disponible, alcance de la actividad informática dentro y fuera de la entidad categoría de clasificación de la información que procesa, determinación de la información sensible para la actividad fundamental de la entidad y los controles establecidos; que brinden los elementos indispensables para evaluar la vulnerabilidad del sistema y los p0rincipales riesgos a que esté expuesto.

4- ¿Qué comprende El Pan de seguridad Informática?

R/
Se instituye como una exigencia para toda las entidades, en el cual deben reflejar las políticas, estructuras de gestión y el sistema de medidas, para la Seguridad Informática, teniendo en cuenta los resultados obtenidos en los análisis de riesgos y vulnerabilidad realizados.El máximo dirigente de cada entidad garantizará, según corresponda a la actividad informática que se desarrolle, que se elabore, ponga en vigor, cumpla y actualice periódicamente.

El Plan de Seguridad Informática y su aplicación serán objeto de aprobación y control por parte de las distintas instancias de la propia entidad.

5- ¿Qué contendrá El Plan de Contingencia?

R/ Para la Seguridad Informática, contendrá las medidas que permitan, en caso de desastres, la evacuación y traslado de los medios y soportes destinados al procesamiento, intercambio y conservación de Informaciones Clasificadas o sensible.Así mismo, contemplará las medidas para la conservación y custodia de los ficheros creados con fines de salvaguarda.

6- ¿Qué se considera Área Vital?

R/ Se consideran áreas vitales aquellas donde se procese, intercambie, reproduzca y conserve Información Clasificada a través de las tecnologías de Información, en dichas áreas se aplicarán las medidas de protección física siguiente;

a) Se ubicarán en locales de construcción sólida, cuyas puertas y ventanas estén provistas de cierres seguros y dispositivos de sellaje, preferiblemente en los niveles más bajos de la edificación, debiendo cumplir con los requerimientos básicos que reduzcan al mínimo las probabilidades de captación de las irradiaciones electromagnéticas que los medios técnicos de computación y comunicaciones emiten
b) A los locales que tengan ventanas que se comuniquen con el exterior de la instalación se le aplicarán medidas que eviten la visibilidad hacia el interior del mismo
c) Aplicar sistema de detección y alarma en todos los lugares que lo requieran

7- ¿Cuáles Áreas se consideran Reservadas?

R/ Se consideran áreas reservadas aquellas donde la información que se procese, intercambie, reproduzca y conserve a través de la tecnología de información sea sensible para la entidad y se aplicarán las normas de protección de acuerdo a las características de cada lugar.

8- ¿Cómo se controlan soportes Informáticos?

R/ Todos los soportes que contengan Información Clasificada serán controladas y conservadas en la oficina de control de la información Clasificada o en el área responsabilizada, según lo establecido para su protección y conservación.
Los soportes pertenecientes a una entidad cuando contengan Información Clasificada o sensible, serán controlados, debiendo reflejar los datos de control en los soporte es removibles que lo permitan, señalizándolos de forma clara y visible, con la categoría de la Información de mas alto valor contenida en los mismos.

9- ¿Diga las funciones del Responsable de Seguridad Informática en cada entidad?

R/

a) Ser responsable de la aplicación y mantenimiento de los planes de seguridad informática y de contingencia
b) Comunicar al Jefe Administrativo de su área cuando en ella no se osean los productos de seguridad informática actualizados y certificados de acuerdo a las normas recogidas en el presente Reglamento y a las condiciones de trabajo del área
c) Apoyar al trabajo del Jefe de Protección y el jefe Administrativo en cuanto al estudio y aplicación del sistema de Seguridad a los sistemas Informáticos, con el fin de determinar las causas y condiciones que propicien violaciones en el uso y conservación de estos sistemas y en la Información que se procese en ellos
d) Proponer y controlar la capacitación del personal a esta actividad con el objetivo de contribuir su conocimiento y cumplimiento de las medidas establecidas en el Plan de Seguridad Informática y en este Reglamento
e) Analizar periódicamente los registros de auditoria a la Seguridad Informática

10 ¿Diga las funciones del administrador de una red, en relación con la Seguridad Informática?

R/ Art. 45: Toda red de computadoras deberá contar para su operación con la existencia de un Administrador que tendrá entre sus funciones básicas:

a) Velar por la aplicación de mecanismos que implementen las políticas de Seguridad definidas en la red
b) Velar porque la misma sea utilizada para los fines que fue creada
c) Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de acciones nocivas que se identifiquen
d) Contar con un mecanismo de coordinación y aviso con el resto de las redes nacionales y el Ministerio del Interior, que permita actuar de conjunto ante la ocurrencia de violaciones