



**Instituto Nacional de Estadística e  
Informática**

**LINEAMIENTOS DE POLÍTICA NACIONAL  
DE SEGURIDAD DE LA INFORMACIÓN  
EN EL ESTADO PERUANO**

**Diciembre 2002**

# INTRODUCCION

El presente documento es una propuesta inicial de lo que pretende ser el desarrollo de la “**Política Nacional de Seguridad de la Información en el Estado Peruano**”,

Una Política de Seguridad de la información es una estrategia frente a los riesgos que pueden atentar contra la confidencialidad, la integridad y la disponibilidad de los recursos informáticos, dichas estrategias se elaboran en base a la identificación de los riesgos tanto internos como externos de toda la infraestructura informática de una institución.

El INEI como ente rector del sistema Nacional de Informática del Estado Peruano, siendo conciente de la dependencia del gobierno con los sistemas de información existentes, en todos los procesos de la administración pública, afirma la necesidad de dar alta prioridad a la seguridad de las operaciones del gobierno y sus respectivos activos informáticos. Para esto requiere que las entidades públicas identifiquen las debilidades y riesgos actuales de seguridad, así como resuelvan la protección a las vulnerabilidades y amenazas futuras.

Para ello se esta trabajando en diferentes componentes :

<b>NORMAS (que es lo que queremos)</b>				
<b>DIRECTIVAS (como lograrlo)</b>				
<b>PUBLICACIONES</b>	<b>PROGRAMAS DE ANÁLISIS DE VULNERABILIDAD</b>	<b>CONVENIOS</b>	<b>CAPACITACION</b>	<b>OTROS</b>

Las Normas son las políticas que se establecen y que nos dicen que es lo que queremos en términos de seguridad de la información. Las directivas apoyan a las normas, mediante la forma de como lograr obtener lo que se plantea como norma o política. Y todo esto descansa sobre las diferentes actividades que realiza el INEI para apoyar la seguridad de la información en las instituciones publicas.

El presente documento presenta las políticas de seguridad de la información a ser tomadas en cuenta por todas las instituciones del Estado Peruano, lo cual implica una serie de recomendaciones con el objetivo de tener las fuentes de información públicas funcionando y atendiendo de una manera segura, lo cual permitirá una continuidad en los servicios informáticos de las instituciones del estado.

## **PLANEACIÓN DE LA TECNOLOGÍA DE INFORMACIÓN**

Un aspecto muy importante es el de la planificación de las tecnologías de la información, muchas organizaciones se han resistido a invertir en tecnologías de seguridad de la información no planificando el desarrollo de estos recursos, y en otros casos existe el paradigma referido a la seguridad informática, en el sentido de que la información se encontrará vulnerable por la presencia creciente de intrusos cibernéticos, si hacemos publica la información.

Ante esta situación cabe indicar que, a pesar de la creciente disponibilidad pública de la información y el aumento del número de intrusos potenciales actualmente, también existen las herramientas de seguridad así como la capacitación en dichos temas, con la finalidad de construir defensas efectivas y mejorarlas continuamente.

Con una planificación integral, anticipada, efectiva, es posible responder rápida y apropiadamente cualquier tipo de riesgo que atente en contra de los sistemas de información, sean éstos por intentos de accesos no deseados, eventos inesperados, o cualquier otra acción que atente contra la integridad o disponibilidad de la información. Algunas veces se logra prevenir la mayoría de ellos minimizando el efecto nocivo de los ataques.

La planeación general de la seguridad de la información, debe ser parte de los objetivos de la Institución debiendo tener en cuenta lo siguiente:

- ≡≡ El plan debe fluir directamente de los planes operativos de la organización.
- ≡≡ El plan debe describir los requisitos empresariales que satisfarán las metas operativas: no es una lista de deseos computarizada.
- ≡≡ Hay que concentrarse en lo que se necesita hacer, no en cómo se hará. Por lo común hay muchas maneras de satisfacer un requisito, y entre ellas hay grandes diferencias en costo.
- ≡≡ Debe haber una justificación clara para cada gasto que se haga. Y, desde el principio, hay que incluir la seguridad en el plan de tecnologías de información.

Las arquitecturas de hardware y software, deben mantenerse simples. Esto ofrece una ventaja importante en materia de seguridad. En el caso de los sistemas múltiples no importa cuán estrechamente estén integrados, estos ofrecen varios puntos de acceso y requieren mayor administración de seguridad y sistemas de apoyo que se traducen en el incremento de costos.

## **Propuesta de Políticas**

Una política de seguridad de la Información es una forma de comunicarse con los usuarios y los Jefes. Las Políticas de Seguridad de la Información establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización.

No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el por qué de ello.

Cada política de seguridad de la información es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus actividades. Invitación que debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la institución.

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

En este sentido la seguridad debe ser construida y fundamentada como parte de la arquitectura del sistema de información de toda institución pública. Las instituciones deben crear roles de seguridad explícitos en las inversiones de tecnología de información y programarlas en los presupuestos. Estas acciones deben ser completamente constantes.

### **1. Planificar la seguridad, tomando en cuenta lo siguiente:**

La planificación de la seguridad es la etapa en donde se realiza la identificación actual de los recursos informáticos, los alcances de los servicios de estos brindan a los usuarios a nivel de aplicaciones, con lo cual se hace una proyección en base al crecimiento de los servicios que se ofrecen, identificando los requerimientos necesarios para implementar y controlar el funcionamiento del mismo. Para lo cual se deben tener en cuenta las siguientes consideraciones.

#### **Acciones**

- a. Demostrar que los costos de los recursos de seguridad están entendidos e incorporados explícitamente en las hojas de planificación del ciclo de vida total del sistema de una manera constante con la dirección de presupuesto para la programación de capital.
- b. Incorporar un plan de seguridad que discuta:

- i. Las reglas de utilización del sistema y las consecuencias al violar dichas reglas;
- ii. Personal y controles técnicos para el sistema;
- iii. Los métodos para identificar, limitar apropiadamente, y administrar los límites de las interconexiones con otros sistemas y los procedimientos específicos para vigilarlos.
- iv. Procedimientos para el entrenamiento de los individuos que tienen acceso permitido al sistema;
- v. Procedimientos para el monitoreo de la eficacia de los controles de la seguridad;
- vi. procedimientos para reportar y compartir con indicaciones apropiadas de las autoridades del gobierno, de intrusiones procuradas y acertadas en sistemas de una institución.
- vii. provisiones para la continuidad de la ayuda en el acontecimiento de la interrupción o del incidente de un sistema.

## **2. Administración del inventario**

Los elementos de Tecnologías de Información (computadoras personales, servidores, tarjetas de red, cables, etc.) y los suministros (programas de computadora, diskettes, etc.) deben inventariarse y asegurarse apropiadamente. frecuentemente, las instituciones reciben grandes cantidades de equipo físico y programas de computadora (computadoras personales, monitores, tarjetas de acceso a la red, bocas de conexión en paneles de control, dispositivos que conectan dos redes de área local, etc.) sin anotar esos artículos en un banco de datos de control de activos, y sin verificarlos cuidadosamente para garantizar que son lo que se pidió y que los artículos están configurados correctamente y funcionan apropiadamente. cuando se pierden los artículos o no funcionan apropiadamente, no hay constancias para demostrar la pérdida o que el sistema no funciona como se requiere. la administración de inventario es un primer paso.

### **Acciones**

- a. En el momento en que se recibe un equipo o componente electrónico, debe establecerse la configuración de cada pieza del equipo físico y cada programa de computadora debe quedar apropiadamente registrado.
- b. El inventario contendrá, una descripción detallada de cada uno de los componentes del sistema, tanto equipo físico como programas de computadora, y de dónde están ubicados (hasta llegar al número de la oficina y escritorio). esta información es de valor inapreciable para la protección de los activos informáticos, la identificación del robo o la

manipulación y la realización de investigaciones efectivas cuando se descubren problemas.

- c. Automatizar mediante una aplicación electrónica el proceso de administración del inventario. En el mercado hay disponibles programas de computadora que verifican la configuración e informan automáticamente acerca de problemas a los administradores de seguridad. estos programas mantienen también un registro de cambios o de mantenimiento del sistema. según se van realizando reparaciones, se introducen mejoras en los sistemas o se les presta mantenimiento, es importante que se deje constancia de tales actividades.
- d. Utilizar cerraduras y tornillos especializados para cerrar las estaciones de trabajo. Con esto se reduce el robo o la manipulación.
- e. Se deberán informar a la alta dirección, de todos los problemas que parezcan sospechosos para proceder a investigarlos.
- f. Dividir en compartimientos el almacenamiento y localización de los suministros y activos cibernéticos, según su costo o la importancia que tengan para la misión de la agencia. A menudo se descuida este aspecto. por ejemplo, algunas instituciones guardan suministros de bajo costo tales como diskettes, en compartimientos muy seguros, en tanto que los activos cibernéticos esenciales, tales como los servidores, quedan sin protección en un área de oficina abierta, y los cables y centros de la red se instalan al descubierto sobre las paredes en lugar de encerrarlos en conductos o esconderlos dentro de los cielorrasos.

### **3. Alinearse a la arquitectura de información de la institución.**

Esta política define la necesidad de considerar dentro de la infraestructura física y funcional de los sistemas de información, el desarrollo de un plan de seguridad en función al crecimiento de esta arquitectura.

#### **Acciones**

- a. Los controles de la seguridad para los componentes, las aplicaciones, y los sistemas deben ser parte integral de la arquitectura tecnológica de los sistemas de información de la institución.

### **4. Tomar control de los riesgos.**

Los riesgos son constantes y se necesita tener los mecanismos necesarios para analizarlos y posteriormente aplicar las estrategias precisas frente a estos riesgos, y no esperar a que ocurran para construir una solución.

## **Acciones**

- a. Establecer un método específico y entendible para evaluar continuamente los riesgos potenciales, con la finalidad de mantener la seguridad en un nivel aceptable, así como los procedimientos para asegurar un control eficaz con los tiempos de respuesta necesarios.
- b. Identificar de ser necesario controles adicionales de seguridad para reducir al mínimo el riesgo potencial de pérdida de los sistemas al promover o permitir acceso público.

## **5. Proteger la privacidad.**

Es necesario el establecimiento de mecanismos que ayuden a proteger la identificación de las personas, que realizan comunicación para acceder al uso de recursos de información de las entidades públicas.

### **Acciones**

- a. Mantener herramientas eficaces para el control de la autenticación, tal como firmas digitales basadas en clave pública, para sistemas que permiten el acceso remoto, en general para los casos de envío de información sensible.
- b. Asegurar que la información personal este respaldada por políticas del gobierno.
- c. Controlar las aplicaciones y la información a que tienen acceso los usuarios y cómo pueden llegar hasta ellas. (por ejemplo, a un usuario se le puede permitir acceso a ciertas estaciones de trabajo en ciertas ocasiones). controlar quién puede abrir cuentas o crear identificaciones de usuarios en un sistema. auditar las cuentas con frecuencia en busca de identificaciones o cuentas que no correspondan a la realidad. tener a mano personas capaces de llevar a cabo una auditoría.

## **6. Mantener estándares en seguridad.**

Los estándares en informática son las recomendaciones técnicas que facilitan una mejor administración y crecimiento de los recursos informáticos de información a nivel nacional.

### **Acciones**

- a. Para la seguridad de las aplicaciones del estado, asegurar el uso de estándares, al implementar productos y herramientas.
- b. Usar productos de seguridad disponibles y probados en el mercado. los productos basados en estándares abiertos han sido probados y aprobados, y se puede entrevistar a sus clientes y

aprender de ellos. incluso si los productos son nuevos, las metodologías usadas para probarlos pueden evaluarse y examinarse los resultados. lo más importante de todo es que los productos estandarizados de la industria están, de modo típico, bien documentados para que los empleen los usuarios y el personal técnico de tecnologías de información. la documentación y el ensayo de seguridad se descuidan frecuentemente cuando las aplicaciones se desarrollan internamente.

## **7. Mantener simple para los usuarios la implementación de los planes de seguridad.**

Si el sistema es muy complicado, los usuarios lo evitarán o tratarán de darle un rodeo, con lo que se anularán las medidas de seguridad y se reducirá su utilidad. las medidas de seguridad modernas pueden ser efectivas sin interferir.

## **8. Desarrollar y cumplir de forma proactiva políticas, procedimientos y sanciones.**

Se deben establecer métodos para tener la certeza de que las políticas de seguridad establecidas, se están cumpliendo correctamente.

### **Acciones**

- a. Diseñar un sistema de seguridad que se base en las necesidades del usuario, la naturaleza de las aplicaciones y la información que se asegura.
- b. Aplicar las medidas de seguridad constantemente, tener políticas de seguridad que no se aplican es peor que no tener ninguna.

## **9. Entrenamiento constante en el uso del plan de seguridad de la institución.**

Consiste en crear formas que aseguren la continuidad de la capacitación y difusión de las políticas de seguridad en todos los niveles de una institución, desde los directivos hasta los operativos.

### **Acciones**

- a. Crear procedimientos de capacitación de acuerdo a los niveles jerárquicos.
- b. Reforzar el adiestramiento mediante el examen y distribución de material noticioso relevante -- por ejemplo, relatos relacionados con ataques cibernéticos o abusos de sistemas.

## **10. Segmentar la información compartida, los sistemas y los usuarios.**

Esta política tiene la finalidad de proteger apropiadamente la información y los sistemas de acuerdo con su valor.

### **Acciones**

- a. Los informes de inteligencia confidenciales deben estar protegidos mediante una seguridad elevada.
- b. La información que es pública puede ser reemplazada fácilmente, no requiere una seguridad refinada. una evaluación objetiva de los sistemas de información mostrará que una cantidad mucho mayor de ellos son públicos en lugar de confidenciales.

## **11. Documentar toda la información relevante al tema de seguridad en las instituciones.**

Esta política consiste en documentar todos los procesos y configuraciones necesarias referidas a temas de seguridad de la información que se implementen en una institución, es decir desde los manuales hasta las procedimientos de aplicación, configuraciones, pruebas realizadas, experiencias obtenidas, entre otros. Sin la respectiva documentación no se tendrá el éxito esperado para lograr la seguridad de la información de una institución.

Una de las amenazas a la seguridad que se descuida con más frecuencia se relaciona con la documentación del sistema. a menudo, la documentación de cualquier tipo se trata con demasiado descuido y es posible encontrarla en oficinas que no son seguras. hay que proteger la información técnica detallada y la que corresponde a los usuarios. puede parecer conveniente y menos costoso preparar documentación que se adapte a todos los usos, pero esto puede resultar peligroso para la seguridad de un sistema. los manuales de usuario que se distribuyen profusamente contienen a menudo grandes cantidades de información técnica que no le sirve de nada al usuario instalado frente a su terminal, pero que puede ser muy valiosa para el intruso cibernético. uno de éstos, armado de información detallada sobre el sistema, puede atacarlo con precisión quirúrgica en lugar de apelar a la fuerza bruta, más fácil de detectar.

### **Acciones**

- a. La alta dirección de cada institución emitirá directivas internas referidas a la documentación de los procedimientos realizados en beneficio de la seguridad de la información.

- b. La jefatura de informática documentara los procedimientos, configuraciones y toda la información necesaria para la continua implementación de la seguridad.
- c. Distribuir la documentación según la necesidad que cada cual tenga de conocerla.
- d. Controlar el acceso a la documentación y adiestrar a los usuarios acerca de cómo protegerla.
- e. Es recomendable, para reducir costos, simplificar la puesta al día y brindar más protección, publicar la documentación en la red en lugar de imprimirla.

## **12. Probar, auditar, inspeccionar sitios e investigar continuamente y al azar.**

La seguridad de la información es una actividad constante y necesita del establecimiento de acciones continuas, por ello es necesario tomar en consideración las siguientes acciones :

### **Acciones**

- a. Realizar de forma periódica análisis de vulnerabilidades de los sistemas de información para protegerse de las amenazas internas y externas.
- b. Usar una metodología para examinar y probar códigos para bloquear las puertas traseras de los sistemas informáticos.
- c. Usar auditoría automática y programas de vigilancia. use programas para verificar cambios en un documento.
- d. Desarrolle y use programas como un modo de identificar atacantes reales o potenciales.
- e. Dé a conocer las amenazas y las respuestas que se les da.
- f. Emprenda siempre acción rápida, constante y apropiada cuando se detectan o informan violaciones a los sistemas de información.
- g. Anuncie con amplitud las medidas disciplinarias tomadas en casos que tengan que ver con la seguridad de la ti.