REPÚBLICA DE COLOMBIA

M I N I S T E R I O D E TR A N S P O R T E

SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

RESOLUCIÓN No. 1926 DE

(09/05/2006)

“Por la cual se reglamenta las Políticas de Seguridad Informática para la Superintendencia de Puertos y Transporte”

EL SUPERINTENDENTE DE PUERTOS Y TRANSPORTE

En uso de sus facultades legales conferidas por la Ley 01 del 10 de enero de 1991 artículo 25; el Decreto 101 del 02 de febrero de 2000; el artículo 6 y numeral 18 del artículo 7 del decreto 1016 de junio 06 de 2000, del Decreto 2741 del 20 de diciembre de 2001, el Decreto 1002 del 31 de mayo de 1.993 y las Leyes 105 de 1.993 y 336 de 1.996.

CONSIDERANDO:

Que La Ley 599 de 2000 en su artículo 197, Castigar a los delincuentes virtuales.

Que el artículo 195 del Código Penal, regula temas como: el acceso abusivo a un sistema Informático.

Que el artículo 148 del código de procedimiento penal, menciona que en una actuación procesal de carácter penal se podrán utilizar los medios mecánicos, electrónicos y técnicos que la ciencia ofrezca y que no atenten contra la dignidad humana y las garantías constitucionales.

Que en virtud de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Definir como **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** para la Superintendencia de Puertos y Transporte como el conjunto de normas, reglas, procedimientos y prácticas que regulan la protección de la información contra la pérdida de confidencialidad, integridad o disponibilidad, tanto de forma accidental como intencionada.

ARTÍCULO SEGUNDO: La Política de seguridad nos debe indicar:

- Qué hay que proteger
- Qué Principios deben tenerse en cuenta

"Por la cual se reglamenta las políticas de seguridad para la Superintendencia de Puertos y Transporte"
"

- Cuáles son los Objetivos de Seguridad a conseguir
- La asignación de cometidos y responsabilidades

La Política de Seguridad busca proteger la información, se basa en los principios de Confidencialidad, Integridad, Disponibilidad, Autenticación, autorización no repudio y auditabilidad, siendo el principio una norma o idea fundamental que rige la Política de Seguridad y que se acepta en esencia. Y los Objetivos son la declaración expresa de la intención de conseguir algo que contribuye a la seguridad de la información, bien porque se opone a una de las amenazas identificadas o bien porque satisface una exigencia de la política de seguridad de la información.

ARTÍCULO TERCERO: La política de seguridad busca proteger el desarrollo del software el hardware, las tecnologías de transmisión de datos a través de comunicaciones y redes, programa general de seguridad Internet incluyendo acceso, uso, confidencialidad administración, conectividad, uso de correos.

El ingreso de nuevos equipos a la red, la existencia de protocolos no necesarios, la mala configuración de equipos activos de red o la de mantenimiento al cableado estructurado y las interfaces de red pueden causar la decadencia del desempeño de la red. Por medio de pruebas, captura de paquetes, análisis de flujo de información y verificación de la configuración de equipos activos de red (switch, routers), podemos ofrecer una solución óptima para depurar y optimizar el funcionamiento de la red.

ARTÍCULO CUARTO*:* AUDITORIA DE SEGURIDAD. La Seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Igualmente, a este ámbito pertenece la política de Seguros. La Seguridad Lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Así, podrán efectuarse auditorias de la seguridad global de una Instalación Informática- Seguridad General-, y auditorias de la Seguridad de un área informática determinada- Seguridad Específica-.

ARTÍCULO QUINTO: Adoptar el manual de seguridad informática el cual establece la protección y seguridad de software, hardware, conexiones entre redes y el uso de correos electrónicos e Internet.

PUBLÍQUESE Y CÚMPLASE

Dada en la ciudad de Bogotá , a los

ALVARO HERNANDO CARDONA GONZÁLEZ
Superintendente de Puertos y Transporte

Proyectó: Oficina Asesora de Planeación, Bernardo Santamaría C
Revisó: Oficina Jurídica, Doris Alba Cuervo Aguilar
C:\Documents and Settings\claudiasepulveda\Escritorio\2006 - 04 Oficina Asesora de Planeacion\04.05 Norma ISO 9001 - 2000\04.05.01 Actas de Seguimiento\Resolución MECI.doc