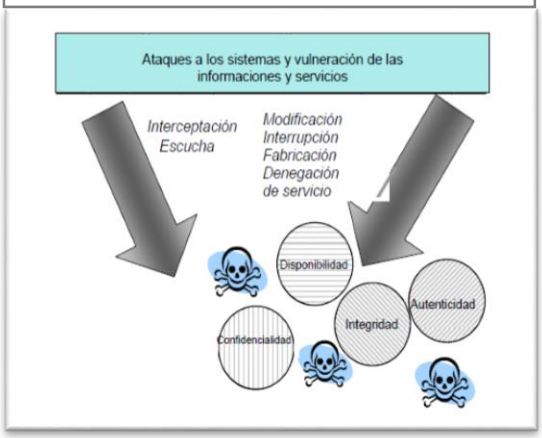
CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA

Ataques a los sistemas y vulneración de la seguridad de los recursos



Según las mediciones realizadas por el Centro de Cibercrimen de Microsoft, en los Estados Unidos, así como por empresas como Symantec, McAfee y Eset, Colombia presenta altos índices de incidentes informáticos, las modalidades de delitos más comunes en nuestro país tienen que ver con robos de identidad digital, de recursos de entidades, empresas y personas, ataques dirigidos contra el Estado y compañías financieras; así como el robo y secuestro de equipos e información pública y privada.

Por esto, el gobierno colombiano, conociendo el alto grado de vulnerabilidad en el que se encuentra el país, se prepara para implementar un nuevo modelo de ciberdefensa y de seguridad digital.

Y aunque Colombia cuenta desde el año 2011, con una política de ciberseguridad y ciberdefensa descrita en el Conpes 3701, la cual creó cuatro organizaciones para la protección interna y externa del país en el ámbito digital, el gobierno anuncia que tanto a nivel oficial como privado se implementarán estrategias para preparar a entidades, empresarios, sistema judicial, Policía, Fuerzas Militares y entes de investigación para prevenir y combatir las amenazas de seguridad informática que puedan afectar a la ciudadanía y a los intereses de la nación.

Con esto, Colombia tendría un sistema de seguridad externa (ciberdefensa) y otro de políticas internas (ciberseguridad). Además reforzará el personal y pie de fuerza en seguridad digital, se destinarán más recursos a los comandos y grupos de investigación de defensa y seguridad digitales, actualizará e incrementará el uso de la tecnología para la lucha contra el cibercrimen y por supuesto, incrementará el presupuesto y el trabajo con expertos privados.

- Los riesgos de un ataque cibernético a las redes interconectadas del país son cada vez más altos: Cuanto más se extienda el uso de Internet en nuestro país y se aumente la dependencia a las infraestructuras y tecnologías informáticas, el nivel de vulnerabilidad se incrementará. Esta situación tiene que ser atendida con el objetivo de evitar situaciones como la que vivió Estonia en el2007.
- La Ciberdefensa y Ciberseguridad son un tema estratégico para el país: Ante el surgimiento de amenazas cibernéticas regulares e irregulares, que están en posición de

amenazar la seguridad nacional de cualquier país, los gobiernos y Fuerzas Militares del mundo han empezado a considerar la Ciberdefensa y la Ciberseguridad como capacidades estratégicas prioritarias a fortalecer en los próximos 10 años.

- El colCERT debe enmarcarse en una Política Nacional de Ciberseguridad y Ciberdefensa en donde participen de manera coordinada el sector público y el privado, con estructuras y financiamiento que permitan su continuo fortalecimiento en el futuro.

INCIDENTES PRESENTADOS EN OTROS PAISES Y LAS ACCIONES QUE HAN TOMADO LOS GOBIERNOS

ALEMANIA

INCIDENTES

- Recibiómilesdeintentosdeespionajecomercialporpartedehackerschinos, que en algunos casos llegaron a bloquear páginas web gubernamentales por varias horas.
- Constantementerecibeataquesporpartede hackersrusosasuredeléctricayferroviaria

ACCIONES TOMADAS

- Recibiómilesdeintentosdeespionajecomercialporpartedehackerschinos, que en algunos casos llegaron a bloquear páginas web gubernamentales por varias horas.
- Constantementerecibeataquesporpartede hackersrusosasuredeléctricayferroviaria

COREA DEL SUR

INCIDENTES

- Sus redes informáticas civiles y militares están bajo continuo ataque; se reporta que mensualmente sufren alrededor de 10.500 intentos de ingresos piratas y de 81.700 contagios con virus informáticos.
- En 2004, hackers chinos y norcoreanos robaron información ultra secreta de sistemas de diferentes agencias gubernamentales.

ACCIONES TOMADAS

- Planea la creación de un Comando Conjunto Unificado de Guerra Cibernética para 2012 con el fin de enfrentar la amenaza creciente de ataques a sus redes informáticas gubernamentales y militares.
- Las entidades civiles han desarrollado un fuerte mecanismo privado de defensa a los ataques, dada la poca eficiencia de las acciones adelantadas en este sentido por parte del Estado.

ESTADOS UNIDOS

INCIDENTES

- En enero de 2009, hackers robaron información ultra secreta del JointStrikeFighteróF-35 (el proyecto de un sistema de armas más costoso en la historia de Estados Unidos).
- El 4 de julio de 2009, deshabilitaron las páginas web del Departamento del Tesoro y de Estado, de la Comisión Federal de Comercio, del Pentágono y de la Casa Blanca.

ACCIONES TOMADAS

- Creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés).
- Este Centro optimiza los esfuerzos hechos por parte de las Fuerzas Militares y otras agencias, y provee al país con la capacidad de defender la infraestructura tecnológica y de conducir operaciones ofensivas.