

Taller Regional sobre Ciberseguridad y Protección de la Infraestructura Crítica

Sección 2: Desarrollo de una Estrategia Nacional

Carlos Achiary
Director de la Oficina Nacional de
Tecnologías de Información
Subsecretaría de la Gestión Pública

Contexto global

- Creciente dependencia de las TICs
- Expansión del Comercio Electrónico
- Desarrollo del Gobierno Electrónico

- Aumento de la actividad ilícita en redes e Internet
- Transnacionalización de los incidentes informáticos
- Ciberterrorismo y ciberguerra

Tendencia internacional

- Protección de las Infraestructuras Críticas
- Capacidades de respuesta a incidentes
- Cooperación internacional
- Interacción entre distintos actores de la sociedad
- Marcos normativos nacionales
- Actividades de concientización

Protección de Infraestructura Crítica

IMPORTANCIA

- Provee una visión estructurada de los recursos y servicios de información estratégicos
- Permite la evaluación de amenazas y vulnerabilidades, la determinación de los riesgos y la implementación de controles
- Es la base para construir un plan nacional de respuesta
- Favorece la estabilidad, tanto a nivel nacional como internacional

Rol del Estado



- Principal receptor/emisor de información
- Custodio de información de los ciudadanos
- Usuario e impulsor de TICs
- Proveedor de información y servicios esenciales
- Regulador a través de normas y reglamentaciones
- Representante de un país

Rol del la ONTI

JEFATURA DE GABINETE DE MINISTROS
DR. ALBERTO ANGEL FERNANDEZ

UAI
Auditoría Adjunta:
Área Legal
Área Contable
Área Informática
Área Operacional

SECRETARIA DE GABINETE Y RELACIONES PARLAMENTARIAS
Lic. Juan Carlos PEZOA

SUBSEC. DE LA GESTIÓN PÚBLICA

SSEC. DE RELACIONES INSTITUCIONALES
Lic. Alberto R. R. PEREZ

D.PUBLICIDAD OFICIAL
DELEGACION LEGAL
DELEGACION TEC.- ADM.

D.G.DE COMUNICACION

D.G.TEC- ADM.
D.N.DE PROG. Y PROY. CON FINANC.EXT.

OF.N. DE EMPLEO PÚBLICO
OF.N. DE INNOVACIÓN DE GESTIÓN

D. DE FORTALECIMIENTO DE LA DEMOCRACIA

D.G. DE ENLACE Y REL. PARLAMENTARIAS

OF. NAC. DE TECNOLOGIAS DE INFORMACION

INAP
DELEGACION TEC-ADM.

Coord de Ceremonial
Coord de Tramitación Téc.
D.G.DE ASES. LEGAL
D. DE ASISTC. NORMAT.
Coord de Asuntos Técnicos

- ✓ Lleva adelante el funcionamiento del Gobierno Nacional
- ✓ Elabora estándares
- ✓ Impone el sistema digital
- ✓ es Autoridad Certificante
- ✓ Entiende en aspectos de seguridad de la información del Estado



- ArCERT
- Cooperación Internacional
- Vinculación con otros sectores
- Generación de un marco normativo
- Actividades de concientización

CREADO	Julio de 1999
AMBITO	Organismos Públicos
OBJETIVO PRINCIPAL	Incrementar los niveles de Seguridad Informática del Sector Público Atención de Incidentes de Seguridad

Cooperación Internacional

- Participación en la Iniciativa de la OEA para la construcción de una red hemisférica de CSIRTs
- Membresía en el FIRST desde 2004
 - Sede del primer Coloquio Técnico en Latinoamérica (2005)
- Contactos regionales para la conformación de CSIRTs
 - Chile, Bolivia, Panamá, Perú, Venezuela
 - Curso para la formación de CSIRTs en áreas de gobierno de Latinoamérica (Buenos Aires - 2004)
- Designación de Expertos en iniciativa de la ITU

Coordinación con otras áreas

ENTIDADES PÚBLICAS

- Organismos Nacionales y Provinciales
- Poder Judicial
- Poder Legislativo

ENTIDADES PRIVADAS

- Cámaras
- Bancos e ISPs
- Público en General

SECTOR ACADEMICO

- Universidades Nacionales
- Institutos de Enseñanza

PLAN NACIONAL DE GOBIERNO ELECTRÓNICO

Decreto 378/05 OBJETIVOS

- Impulsa la utilización de las TICs para brindar mejores servicios y mejorar la gestión Pública
- En cuanto a seguridad
 - Obliga a establecer políticas de seguridad
 - Crea un Portal de autenticación para la identificación de los habitantes, ciudadanos y usuarios que deban operar con el Estado

Marco Normativo Nacional

POLITICAS DE SEGURIDAD PARA EL ESTADO NACIONAL

OBJETIVOS

- Establecer un marco normativo para gestionar la seguridad de la información (DA N° 669/2004)
- Proteger adecuadamente la información en poder del Estado
- Promover la concientización a nivel de toda la organización
- Asignar responsabilidades

Marco Normativo Nacional

POLITICAS DE SEGURIDAD PARA EL ESTADO NACIONAL



Relevamiento sobre necesidades de los Organismos en materia de Seguridad de la Información



Redacción, en conjunto con otros Organismos, un Modelo de Política de Seguridad



Modelo aprobado el 03/08/2005 por Disposición ONTI N° 06/05, sobre la base de la Norma IRAM/ISO 17799



Capacitación y asistencia para redacción de políticas



Procedimientos y documentos modelo publicados en sitio de acceso a organismos públicos

Marco Normativo Nacional

PROYECTO DE LEY SOBRE DELITO INFORMÁTICO

- Acciones ONTI
- Informe a HCD y HCS**
 - Participación y colaboración en reuniones de trabajo del Congreso**
 - Cursos y Jornadas de difusión para la APN**
 - Reuniones con otras entidades**
 - Presentaciones en eventos**

Concientización

- Elaboración de documentos específicos (NTP, seguridad en desarrollos web, etc.) y sobre temas de alcance general (correo electrónico, “phishing”, etc.)
- Cursos de capacitación para técnicos del Estado y usuarios en general
- Participación en eventos y programas de radio y televisión
- Sitio Web y Lista de Seguridad

Logros alcanzados

- Grado importante de conciencia sobre la importancia del tema
- Designación de un equipo dentro de la estructura gubernamental para la respuesta a incidentes
- Establecimiento de un marco normativo en seguridad para el Sector Público
- Avance en la legislación nacional sobre delitos informáticos

Próximos pasos

- Profundizar la cooperación, tanto dentro como fuera del país, en la región y a nivel mundial
- Avanzar en el desarrollo de un plan de acción para la protección de la infraestructura crítica del país, en conjunto con los sectores involucrados

¡Muchas Gracias!

Preguntas y Comentarios

www.sgp.gov.ar

www.arcert.gov.ar

info@arcert.gov.ar