ISNN 999-4605

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

58
EDICIÓN

FORO e-GOBIERNO OEA | BOLETÍN

OCTUBRE 2010

e-Gobierno y Seguridad de Información

IDRC CRDI

Canadian International Development Agency
Agence canadienne de développement international

Canada

TABLA DE CONTENIDO

CRÉDITOS

Miguel A. Porrúa
Coordinador e-Gobierno, OEA

José Luis Tesoro
Responsable Foro e-Gobierno, OEA

Javier Sáenz Coré
Indagación de enlaces Web, OEA

Daniela Paoli
Oficial e-Gobierno, OEA

EDITORIAL

Si consideramos al e-Gobierno como una nueva forma de relación entre gobiernos y ciudadanos, en la cual las TIC se constituyen en herramienta fundamental para proveer información y servicios, percibimos como una amenaza a cualquier factor que pueda inhibir o bloquear la efectividad de esa función herramental. Tales factores podrían provenir de los fabricantes de las herramientas, del prestador, del operador, del usuario, de terceros o del entorno.

Si bien puede afirmarse que los mayores factores de vulnerabilidad para la efectividad del e-Gobierno no residen en las tecnologías, sino en la actitud y disposición de los gobiernos como proveedores de información y servicios, es en la faz tecnológica donde se manifiestan los mayores avances -estándares, protocolos, métodos, reglas y herramientas- para proteger la infraestructura informativa, lógica y física del e-Gobierno.

El mercado ofrece múltiples opciones para prevenir y mitigar las amenazas provenientes de operadores, usuarios, intrusos, programas maliciosos, así como de otras eventuales fuentes de siniestros. Las opciones se extendieron notoriamente a raíz de la ampliación del rango de amenazas emergentes de la denominada Web 2.0, previéndose una evolución hacia las nuevas amenazas asociadas a la digitalización semántica, en que el blanco de ataques se proyecta al significado del contenido virtual en la Web 3.0 (Web semántica).

Este número del Boletín, dedicado a “e-Gobierno y Seguridad de la Información” tiene el propósito de aportar elementos de juicio acerca del estado de la cuestión, de los marcos normativos y operacionales que se van gestando en la materia, así como de algunas experiencias transitadas en los países de las Américas.

El equipo de e-Gobierno de la OEA asigna gran relevancia a la cuestión de la ciber-seguridad para el avance sostenido del e-Gobierno y promueve el intercambio de experiencias entre los gobiernos de las Américas para proteger estratégicamente la Integridad de la información y la disponibilidad de los servicios de e-Gobierno.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA)
Secretaría de Asuntos Políticos (SAP)
Departamento para la Gestión Pública Efectiva

TEMA DEL MES
GOBIERNO ELECTRÓNICO Y SEGURIDAD DE LA INFORMACIÓN

Entrevista a Belisario Contreras

Administrador Asistente de Proyectos del Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA)

Por José Luis Tesoro

1.- ¿Cuáles son las principales amenazas a la Seguridad Cibernética en las Américas?

Los Estados Miembros de la Organización de los Estados Americanos (OEA), a través de la "Estrategia Interamericana Integral de Seguridad Cibernética", han reconocido que si bien la Internet ha impulsado e impulsa un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el Hemisferio, también ha generado nuevas amenazas que ponen en peligro la seguridad de los Estados Miembros, del sector privado, de la sociedad civil y de los usuarios de Internet en general.

Es imprescindible tomar clara conciencia de que Internet es un medio de comunicación en el que, si no se adoptan las medidas necesarias, la información puede ser manipulada para atentar contra la seguridad de los gobiernos y de los usuarios de la red. Entre los casos de amenazas más comunes podemos encontrar el terrorismo cibernético, el sabotaje a través de Internet, el espionaje y los delitos como fraude y robo de identidad.

2.- ¿Qué pueden hacer la OEA y sus Estados Miembros para contrarrestar estas amenazas?

De hecho ya se está trabajando intensamente para contrarrestar las referidas amenazas. Con la promulgación de la Estrategia Interamericana de Seguridad Cibernética, una iniciativa única a nivel regional, los Estados Miembros establecieron ciertos mandatos para poder desarrollar medidas eficaces para prevenir, tratar y responder a los ataques cibernéticos, luchar contra la delincuencia cibernética y proteger la infraestructura crítica asegurando las redes informáticas. Estos mandatos fueron asignados al Comité Interamericano contra el Terrorismo (CICTE), a la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) y a la Comisión Interamericana de Telecomunicaciones (CITEL), respectivamente. Desde la adopción de esta Estrategia, estas tres entidades han venido implementando diversas iniciativas y apoyando a los Estados Miembros a través de capacitación.

En el caso de la Secretaría del CICTE, siguiendo el mandato que los Estados Miembros de la OEA le encomendaron a través de la Asamblea General, el programa de Seguridad Cibernética ha venido promoviendo la creación de Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRTs, por sus siglas en inglés) gubernamentales en las Américas, y al mismo tiempo se ha estado conformando una Red Hemisférica de CSIRTs y Autoridades en Seguridad Cibernética. A la fecha, contamos con 15 CSIRTs que han sido designados oficialmente por los Estados Miembros y casi 100 integrantes de la Red Hemisférica. Quisiera resaltar que esta Red de contactos es otra iniciativa única a nivel regional en materia de seguridad cibernética, que esperamos pueda promover el aumento y la efectividad del intercambio de información, experiencia y herramientas entre quienes trabajan en seguridad cibernética a nivel nacional.

3.- ¿Cuán importante es la concienciación y la capacitación en materia de Seguridad Cibernética en los gobiernos y en su relación con los ciudadanos?

Es imprescindible que los gobiernos implementen programas de concienciación en seguridad cibernética para la sociedad civil. La cultura en seguridad cibernética debe ser difundida y desarrollada, especialmente porque en el mundo en que vivimos todo está cada vez más conectado a las tecnologías de la información y a Internet.

Es importante tener en cuenta que al beneficiarnos con los recursos de las redes públicas de datos como Internet y de la infraestructura tecnológica interconectada, también debemos estar preparados para escenarios negativos como el delito, el terrorismo y la guerra, lo cual exige la participación de los gobiernos como promotores de mecanismos de prevención, reacción y defensa.

4.- ¿Cuáles son los desafíos que han encontrado en el área de Seguridad Cibernética en las Américas y qué acciones se están realizando para enfrentarlos?

A lo largo de estos años, la Secretaría del CICTE, a través de la Red Hemisférica de CSIRTs y Autoridades en Seguridad Cibernética, ha identificado desafíos a nivel nacional y regional. Desde el punto de vista nacional podemos observar los siguientes desafíos: a) falta de conciencia sobre seguridad cibernética en los niveles políticos, b) ausencia de un marco nacional de seguridad cibernética y falta de efectiva coordinación interinstitucional, c) falta de apoyo para el personal técnico de los países, y d) falta de continuidad en los proyectos relacionados con la seguridad cibernética. Desde una perspectiva regional, los desafíos que hemos identificado son: a) inadecuadas líneas de comunicación entre las autoridades regionales, b) asimetría entre los niveles de capacidad de distintos Estados Miembros, y c) ausencia de estándares regionales en lo relativo a los CSIRTs gubernamentales.

En el caso particular del CICTE, desde hace tres años se ha venido realizando una intensa campaña de concienciación y capacitación en la materia. Esta Secretaría ha venido desarrollando continuos esfuerzos, a través de cursos y talleres, con el propósito fundamental de proveer de herramientas a los Estados Miembros de la OEA para prevenir y responder ante posibles incidentes de seguridad cibernética.

5.- En su opinión: ¿Hacia dónde avanzará la Seguridad Cibernética en los próximos años?

Creemos que habrá una mayor conciencia sobre la importancia de la temática. Esperamos que, durante los próximos años, muchos más Estados adopten legislación contra el delito y crimen cibernético, una tarea que la REMJA ha venido acompañando. Al mismo tiempo confío en que, con el apoyo de la OEA, seguirá incrementándose el número de CSIRTs y

la cooperación entre los gobiernos será mucho mayor. Es importante tener en cuenta que el mundo cibernético no entiende de fronteras, y que la cooperación e intercambio de información y buenas prácticas será crucial para el buen manejo de la seguridad cibernética de los países. En mi opinión, el éxito de cualquier programa de seguridad cibernética -en el país que sea- estará ligado al éxito de las buenas relaciones y alianzas con otros países en lo que respecta al mundo cibernético.

Entrevista a Mara Irene Misto Macías

Gerente Principal de Seguridad de la Información, Banco Central de la República Argentina

Por José Luis Tesoro

1.- ¿Cuáles son los principales riesgos y amenazas para la seguridad en el ámbito del Gobierno Electrónico?

Cuando un organismo gubernamental ofrece sus servicios fuera del entorno controlado de la organización, a través del uso de las TIC, aumentan las amenazas y los riesgos sobre los activos informativos. Si bien éstos pueden mitigarse, no se dispone de control sobre la totalidad de los factores y amenazas externas.

El impacto que puede producir la materialización de estas amenazas sobre los organismos públicos es significativo, pues no sólo afecta cuestiones administrativas, comerciales o financieras sino que puede provocar daños irreparables en la imagen y reputación de la tecnología utilizada, del organismo y de la confiabilidad de éste ante el ciudadano.

Como en los procesos de toda organización, antes de identificar los riesgos, amenazas y vulnerabilidades, así como de definir posibles estrategias de prevención y protección, se debe determinar la importancia, sensibilidad o criticidad de la información que se procura resguardar.

Las soluciones técnicas de seguridad no son suficientes sin una visión integral de los procesos y los riesgos, precisamente porque fuera de la organización hay menos oportunidad de control y los efectos de una medida no se limitan a lo meramente técnico, administrativo o comercial.

Los principales riesgos y amenazas a la seguridad en el ámbito del Gobierno Electrónico no difieren técnicamente de los existentes en los servicios ofrecidos por otros ámbitos, pero existen cuatro componentes de análisis que deben ser tratados de manera diferenciada:

a) Agentes de amenaza: se trata de aquellos individuos u organizaciones propensos a materializar las amenazas. Este factor es particularmente distinto a otros casos, porque las motivaciones asociadas a generar un daño a un servicio ofrecido por un organismo público responden a un perfil distinto del atacante y de los posibles ataques.

b) Activos de Información: debe identificarse y clasificarse la información crítica y determinar objetivamente el efecto de un eventual daño de manera integral. El efecto negativo de amenazas materializadas no se limita al daño técnico. La confiabilidad de un servicio público puede afectar la calidad de la relación de los ciudadanos con sus gobernantes y con otros servicios públicos y privados asociados.

Por ejemplo, la insuficiente confiabilidad de un Banco Central tiene un efecto negativo sobre la confiabilidad del conjunto del sistema financiero.

c) Visión estratégica: la seguridad debería verse como un componente que -considerado en tiempo y forma- facilita a las organizaciones un desarrollo apropiado. Las principales amenazas internas a la protección de los activos de información residen en la carencia de una visión estratégica de la seguridad, el insuficiente involucramiento de la dirección y la falta de análisis integral del riesgo.

d) Implementación de contramedidas: en materia de seguridad no es suficiente tener buenas soluciones, sino asegurar que éstas funcionen efectivamente cuando se las requiere. El proceso de seguridad es esencialmente preventivo y transcurre a lo largo de todo el ciclo de vida de un servicio y no como un proceso reactivo posterior a un siniestro. Por otra parte, no existen soluciones definitivas, sino que se requiere una constante observación y actualización en relación a amenazas y vulnerabilidades en constante evolución.

2.- ¿Podría referirse en forma genérica a algunos casos de problemas de seguridad y sus consecuencias?

Cuando se trabaja en entornos de servicio externo, se transporta información por diferentes canales e infraestructuras fuera del ámbito de control de las organizaciones, lo que obliga a mantener un fuerte control sobre la información intercambiada entre los distintos puntos y sobre la infraestructura interna que recibe las peticiones del mundo exterior.

Los ataques más comunes se orientan a la denegación de servicios y los efectos buscados por estos ataques consisten principalmente en inhabilitar los servicios que presta la organización comprometiendo el acceso a información disponible para usuarios externos.

Otro ataque que viene creciendo a ritmo exponencial es el phishing, que está orientado a la sustracción fraudulenta de datos confidenciales de usuarios,. En este caso el atacante, mediante técnicas de engaño, se hace pasar por una persona o empresa confiable en una aparente comunicación oficial electrónica (correo, mensajería instantánea, llamado telefónico, entre otros) tratando de obtener datos confidenciales tales como claves de usuario, número de tarjeta de crédito, de cuenta bancaria u otros análogos. Este tipo de ataque compromete la seguridad de los datos personales de usuarios, a quienes puede producir daños financieros, robo de identidad, u otros perjuicios.

Estas amenazas exigen fortalecer el trabajo de concienciación con nuestros usuarios, los mecanismos de prevención en el acceso desde el exterior a la red interna, la actualización de los recursos técnicos y humanos, así como reducir la exposición de información sensible.

3.-. ¿Cuáles son las líneas de acción más difundidas para contribuir a la seguridad en el ámbito del e-Gobierno?

Promovemos cuatro principios básicos para la gestión de seguridad en cualquier ámbito y que resultan aplicables al e-Gobierno:

a. Gestión de Riesgo

Promover la gestión del riesgo a través de los recursos técnicos, humanos y organizacionales suficientes para una administración integral de los riesgos en los recursos, sistemas y redes de información, a partir de una visión holística de los procesos de la organización, un análisis e identificación de los principales activos de

información, sus amenazas y vulnerabilidades. Es necesario contar con procesos formales y periódicos de evaluación de riesgos que permitan establecer los niveles de exposición al daño o corrupción de la infraestructura de seguridad, los sistemas y las redes, así como ayudar en la selección de los controles apropiados para mitigar los riesgos determinados, de acuerdo con la importancia particular de cada activo.

b. Gestión de la Seguridad de la Información

Contar con procesos formales para la gestión de la seguridad de los recursos, sistemas y redes de información. Estos procesos incluyen la participación y responsabilidad activa de los principales referentes de la organización, su incorporación en la estrategia organizacional, la determinación de funciones y responsables de las tareas operativas, los planes y acciones para la protección de los activos de información y una metodología de trabajo basada en la planificación de las acciones, la ejecución efectiva de las tareas determinadas, la verificación e informe de los resultados y la mejora continua.

c. Programa de Seguridad

Contar con un Programa de Seguridad que incluya la definición y ejecución ordenada y verificable de planes de seguridad estratégicos, tácticos y operativos en la implementación, control y seguimiento de contramedidas. Estos planes deben reflejar y adaptarse a los resultados de la evaluación de riesgos de seguridad desarrollados periódicamente en la organización, estableciendo las directrices y procedimientos técnicos y operativos necesarios para mitigar el riesgo de manera oportuna y regular.

d. Manejo de Incidentes de Seguridad

Disponer de los recursos necesarios para identificar, detectar, contener y tratar los eventos de seguridad de los que sea objeto la infraestructura de sistemas y redes de información. Asimismo, establecer las tareas formales para documentar y reportar incidentes, así como para actualizar los recursos preventivos y correctivos existentes o planificados.

4.- En su opinión ¿Hacia dónde avanza la Seguridad de la Información en el ámbito del Gobierno Electrónico?

Se debería pensar en una adecuación funcional de la seguridad de la información, promoviendo un rol estratégico de servicio y acompañamiento a las iniciativas de e-Gobierno. Dado que no existe un entorno que pueda garantizar un 100% de seguridad, antes de impedir la evolución de los servicios de e-Gobierno hacia nuevos escenarios tecnológicos, debemos ser capaces de advertir no sólo los riesgos de cada implementación, sino también de sumar propuestas para acompañar esas implementaciones con niveles de seguridad que no afecten al propósito estratégico de las iniciativas.

Por otra parte, los responsables de seguridad deberían involucrarse y ser involucrados desde la gestación de los proyectos hasta su implementación, en un marco de colaboración que haga de la seguridad un servicio que genera valor agregado y no un obstáculo para concretar los proyectos. Su rol controlante debe flexibilizarse hacia la figura del consejero, asesor y generador de alternativas viables y seguras.

5.- ¿Cuán importante es la concienciación y la capacitación en materia de Seguridad de la Información en los gobiernos y en su relación con los ciudadanos?

No es posible mantener en el tiempo la calidad de los servicios de seguridad si los planes de seguridad carecen de programas de concientización y de capacitación como componentes insoslayables.

La seguridad es tanto una necesidad para las organizaciones públicas, como para los ciudadanos que utilizan sus servicios. En seguridad solemos abordar el análisis de vulnerabilidad intentando detectar el eslabón más débil de la cadena. Dado que el componente humano es generalmente el más débil de los factores, es el que requiere mayor atención a través de acciones sistemáticas de concienciación, entrenamiento y capacitación.

Esto exige también desarrollar habilidades de comunicación efectiva como característica fundamental del personal dedicado a la seguridad. A estas alturas, cuando hablamos de soluciones de seguridad de la información no podemos limitarnos a conceptos meramente técnicos. Los procesos organizacionales son liderados esencialmente por personas y las tecnologías deben adecuarse y acompañar las fortalezas y debilidades de las personas para usarlas de manera apropiada.

Entrevista a Eduardo Wallier Vianna

Responsable por la Coordinación General del Tratamiento de Incidentes de Seguridad en Redes de Computadores del Gobierno Federal de Brasil (CGTIR Gov)

Por José Luis Tesoro

1.- ¿Cuáles son los principales riesgos y amenazas para la seguridad en el ámbito del Gobierno Electrónico?

El preservar la seguridad de la información en organizaciones insertas en ambientes interconectados implica hoy una tarea cotidiana y permanente que exige gran estudio, análisis y dedicación. Tanto las organizaciones públicas como las privadas padecen constantes y diferentes formas de ataques cuando ponen servicios e informaciones a disposición de la sociedad a través del uso intensivo de las TIC.

En ese contexto, pueden verificarse algunos factores que contribuyen a acrecentar la inseguridad en el ámbito del e-Gobierno:

- lanzamiento de nuevos productos y servicios para Internet que son adoptados casi inmediatamente sin la debida evaluación mínima de los requisitos de seguridad;

- facilidad para obtener y utilizar herramientas de ataque, con uso de interfaces gráficas y scripts prefabricados para invasión y desarrollo de "artefactos" de software malicioso (malwares), lo que resulta en un significativo aumento de la cantidad de potenciales invasores que no necesitan ya siquiera disponer de conocimientos computacionales avanzados;

- ampliación y potenciación de la capacidad de causar perjuicios de los nuevos malwares y de las técnicas de ataque, por ejemplo la diseminación/utilización en gran escala de redes de máquinas infectadas (botnets);

- diseminación de páginas falsas, muy semejantes a las originales de e-Gobierno, induciendo al ciudadano a entregar sus datos personales o empresariales a individuos no acreditados y malintencionados; y

- creciente utilización de Internet como herramienta de manifestación de reclamos y desagravios políticos, sociales, económicos, religiosos, etc.

2.- ¿Podría hacer una referencia genérica a algunos casos de problemas de seguridad y sus consecuencias?

Dentro de un verdadero universo de problemas, podemos destacar algunos hechos que facilitan la acción de individuos malintencionados; por ejemplo: desfiguración de sitios web institucionales, indisponibilidad de servicios, re-direccionamiento hacia páginas falsas o acceso indebido a bases de datos gubernamentales.

Cabe señalar que, debido a las ansias por responder prontamente a presiones de la sociedad y alinearse al contexto internacional, la velocidad de desarrollo de las aplicaciones y programas para Internet no es acompañada comúnmente por medidas de seguridad adecuadas y robustas. En muchos casos, la presión por implementar rápidamente la prestación de un servicio o de determinada información no permite probar ni validar exhaustivamente las soluciones, las cuales exhiben frecuentemente vulnerabilidades en su desarrollo e implementación, así como un deficiente mantenimiento y actualización en términos de seguridad.

Otro factor relevante se asocia a la constante actualización de los contenidos informativos directamente por parte de los contenidistas, lo que implica habilitar compartimentos y accesos privilegiados a los sistemas a personas que normalmente carecen de conocimientos técnicos de TIC y de seguridad, con la consecuente generación de vulnerabilidades.

Por último, si bien es ya es una práctica habitual el uso del certificado personal digital (CPD electrónico) para acceder a ciertos datos sensibles (por ejemplo: https://cav.receita.fazenda.gov.br/scripts/CAV/login/login.asp), en la actualidad cualquier usuario puede acceder a la mayor parte de los servicios de e-Gobierno sin necesidad de identificación inequívoca (anonimato virtual).

3.- ¿Cuáles son las líneas de acción más difundidas para contribuir a la seguridad en el ámbito del Gobierno Electrónico?

En este aspecto deseo destacar la puesta en marcha del Grupo de Trabajo sobre Seguridad (GT Seguridad), como componente de la arquitectura e-PING (Patrones de Interoperabilidad de Gobierno Electrónico Brasileño). La arquitectura e-PING define un conjunto mínimo de premisas, políticas y especificaciones técnicas que regulan la utilización de las TIC en el Gobierno Federal, estableciendo las condiciones de interacción con los demás Poderes y esferas de gobierno y con la sociedad en general.

Con la finalidad de organizar la definición de los patrones, la arquitectura e-PING fue segmentada en cinco componentes (“Interconexión”, “Seguridad”, “Medios de Acceso”, ”Organización e Intercambio de Información” y “Áreas de Integración para e-Gobierno”), creándose para cada uno un grupo de trabajo específico compuesto por técnicos actuantes en órganos del gobierno federal. Esos especialistas en cada componente son responsables por la elaboración de las correspondientes políticas y especificaciones técnicas para ser adoptadas por el gobierno federal. Como integrante del GT Seguridad, estoy observando, durante este año, un efectivo desarrollo de los patrones de seguridad de TIC, particularmente en lo relativo a:

- Seguridad de IP
- Seguridad de Correo Electrónico
- Desarrollo de Sistemas
- Servicios de Red

Cabe destacar también la ampliación del uso de certificados digitales como un documento electrónico por parte de las empresas (personas jurídicas). Con dicha constancia digital -cuya validez jurídica está sustentada por Ley- las empresas pueden realizar sus transacciones por Internet con plena seguridad, canalizando por vía electrónica diversos documentos con validez legal y reconocimiento de firma, sin necesidad de convertirlos a soporte papel.

4.- ¿Hacia dónde avanza en Brasil la Seguridad de la Información en el ámbito del Gobierno Electrónico?

En relación a los avances, me referiré a dos actividades distintas pero complementarias y asociadas directamente a la seguridad de la información y al e-Gobierno.

La primera es la construcción de un "Marco civil de Internet", con la participación de toda la sociedad. Para ello se abrió un proceso colaborativo de discusión y debates por Internet (ver http://culturadigital.br/marcocivil/) y se organizará jurídicamente –con fuerza de ley- la utilización de la Internet en el país. El proyecto de ley resultante del proceso reunirá reglas para determinar derechos, deberes y responsabilidades de internautas, proveedores de acceso, así como la actuación del Estado en el ambiente virtual.

La segunda actividad, originada en el gobierno federal, a través del Gabinete de Seguridad Institucional de la Presidencia de la República (GSIPR), se dirige a regular la Gestión de Seguridad de la Información y Comunicaciones en el ámbito de los órganos y entidades de la Administración Pública Federal, directa e indirecta. Esta reglamentación tomó impulso a partir de 2008 y ya abarca diversas áreas vinculadas a la seguridad de la información; por ejemplo:

Elaboración de Políticas de Seguridad, Gestión de Riesgos, Tratamiento y Respuesta a Incidentes en Redes de Computación, Controles de Acceso, entre otras (ver ejemplos de normas en: http://dsic.planalto.gov.br/legislacaodsic/53).

5.- ¿Cuán importante es la concienciación y la capacitación en materia de Seguridad de la Información en los gobiernos y en su relación con los ciudadanos?

Permítame basar mi respuesta en dos hechos recientes del contexto brasileño:

a. En relación a los pequeños y medianos emprendedores de Brasil, se constató que el 93% utilizan Internet, lo que muestra una elevada inclusión digital por parte de las pequeñas empresas.

b. El Plan Nacional de Banda Ancha (PNBL), lanzado por el Gobierno Federal en mayo del corriente año, tiene por objetivo universalizar en el país el acceso a la Internet de banda ancha -de bajo coste y alta velocidad- llevándola a 4.278 municipios, aumentando el número de domicilios con Internet desde los actuales 13,5 millones a 35 millones en 2014, lo que implica alcanzar prácticamente al 90% de la población brasileña.

Estas excelentes noticias implican enormes desafíos para el área de seguridad. Sintéticamente, basta inferir que gran parte de esos nuevos ingresantes al ambiente virtual y -como consecuencia- potenciales usuarios del e-Gobierno, carecen de conocimiento sobre el uso seguro de la Internet. Creo que los programas de concienciación, entrenamientos específicos y campañas de sensibilización, por parte del gobierno y de las empresas proveedoras de Internet, serán herramientas fundamentales para que esos nuevos usuarios no se constituyan en potenciales víctimas de individuos y grupos malintencionados.

6.- ¿Desea agregar algún aspecto adicional?

Deseo agradecer esta oportunidad de expresar algunas ideas sobre seguridad de la información y concluir ratificando que, en los últimos años, los órganos públicos vienen implementando y consolidando redes locales cada vez más amplias de computadores, como exigencia para sustentar el flujo creciente de informaciones, así como para que sus colaboradores y la sociedad accedan a los servicios disponibles por Internet para desempeñar sus funciones y para satisfacer sus necesidades como ciudadanos.

Creo, como ya fue declarado por varias autoridades brasileñas, que el principal foco del e-Gobierno debe ser promover la ciudadanía mediante una vasta gama de servicios, orientaciones e informaciones relevantes para el ciudadano, como puede verificarse en el portal http://www.e.gov.br/.

Sin embargo, con una mirada más técnica y crítica, puede percibirse también que el e-Gobierno se ha constituido en sinónimo de modelo de competencia y de gobernanza estatal, incluso con informes de entidades internacionales en los que se clasifica y califica a los países de acuerdo con los servicios de e-Gobierno ofrecidos a sus ciudadanos. Estos hechos, en cierta forma, presionan a los administradores públicos para acelerar excesivamente la accesibilidad de servicios a la población, en detrimento de la complejidad de la maquinaria pública y de las especificidades técnicas de seguridad. En consecuencia, a veces se verifica –lamentablemente- en el área de e-Gobierno cierto descuido de algunos pilares básicos de la seguridad de la información: disponibilidad, confidencialidad, autenticidad e integridad.

Entrevista a Eduardo Carozo Blumsztein

Gerente de Seguridad de la Información de la Administración Nacional de Telecomunicaciones (ANTEL) y Director Ejecutivo CSIRT-ANTEL, Uruguay

Por José Luis Tesoro

1.- ¿Cuáles son los principales riesgos y amenazas para la seguridad en el ámbito del Gobierno Electrónico?

Desde una perspectiva global, los gobiernos modernos necesitan, cada vez más, tener interacciones cotidianas con el ciudadano, y las TIC les permiten desarrollar propuestas novedosas, inclusivas y sobre todo universales. Preveo que este tipo de interacciones están llamadas a convertirse en la más frecuente y efectiva forma de comunicación y provisión de servicios hacia y para el ciudadano.

Las agendas de transición hacia la Sociedad de la Información incluyen y destacan, en la mayor parte de los países de la región, el desarrollo de herramientas de e-Gobierno en todos los niveles de gobierno; nacional, departamental, local, institucional, etc.

En la medida que los gobiernos adoptan soluciones de e-Gobierno (por ejemplo, para agilizar trámites, centralizar información, estandarizar procesos, realizar transacciones económicas, calcular impuestos, promover emprendimientos, analizar políticas públicas, etc.), las mismas resultan cada vez más valiosas para los ciudadanos, empresarios, políticos, y.... más atractivo es quebrar la seguridad, para perpetrar robos, fraudes o afectar la provisión de servicios esenciales.

Los mayores riesgos que provocan en Latinoamérica parecen ser los robos de identidad, los fraudes financieros (en transacciones económicas), la pérdida de confidencialidad de datos personales, y en forma más limitada (por el acotado desarrollo tecnológico en robótica y control a distancia) exposición a problemas de indisponibilidad o destrucción de infraestructuras críticas.

2.- ¿Podría referirse en forma genérica a algunos casos de problemas de seguridad y sus consecuencias?

La región sufre actualmente ataques de diversos tipos. El más común es el intento de robar información de tarjetas de crédito, a través de técnicas de "*phishing*" contra organizaciones financieras o de venta de servicios por Internet. También han habido pérdidas cuantiosas contra servicios de *Home Banking*; sobre todo en los países de Centroamérica y el Caribe. Se han detectado ataques enfocados a la privacidad de personas de alta exposición pública quebrando sus contraseñas y accediendo a toda la información de sus casillas de correo, servicios de salud o redes corporativas. Son frecuentes también las amenazas de bomba o atentados a organizaciones o personas (por ejemplo empresas de aviación) a través de medios electrónicos, existen variados ataques de "*defacing*" (desfiguración) de sitios Web, también ataques de denegación de servicios distribuidos, etc.

La región de América Latina y el Caribe, tiene grupos activos de individuos bien entrenados que se benefician de un menor grado de seguridad relativo en las entidades privadas y de gobierno.

3.- ¿Cuáles son las líneas de acción más difundidas para contribuir a la seguridad en el ámbito del e-Gobierno?

En primer lugar, la plataforma de soporte del e-Gobierno debe ser diseñada con políticas de seguridad en profundidad, es decir, todo equipamiento que se utilice en la transacción con el ciudadano o empresa (incluido la pc del usuario final) debe cumplir con ciertos estándares mínimos de seguridad.

Además de securitizar los servidores web, las bases de datos, de colocar firewalls y herramientas de detección de intrusos con las mejores prácticas disponibles, es necesario "entrenar" a los ciudadanos para el correcto uso de los sitios, sobre todo enfocándose en los riesgos a los que se exponen desde sus propias instalaciones domiciliarias o de oficina.

Si bien pueden lograrse buenos comportamientos de la plataforma securitizando todos los componentes sobre los que tenemos derechos de administrador (y eso es necesario), debe tenerse en cuenta que un usuario "desprolijo" que -por inconductas de seguridad- permita que otra persona se apodere de su información de autenticación, puede provocar un serio incidente de seguridad.

En definitiva se debe mantener al ciudadano informado y entrenado sobre los riesgos que conlleva convivir con Internet. Esto en general no es contemplado por los gobiernos. También debe alertarse al usuario/ciudadano contra las prácticas de ingeniería social, de amplia difusión en nuestra región.

Por otra parte, los incidentes de seguridad van a ocurrir y es necesario que el ciudadano sepa dónde reportar el incidente lo antes posible, para que el mismo sea mitigado rápidamente.

En los últimos años los países de la mano del CICTE de la OEA y otras organizaciones internacionales como el Proyecto Amparo de LACNIC, están promoviendo la creación de Centros de Respuesta nacionales públicos y privados para enfrentar este tipo de situaciones y apoyar a organizaciones y personas bajo ataque.

4.- En su opinión: ¿Hacia dónde avanza la Seguridad de la Información en el ámbito del e-Gobierno? La Seguridad de la Información toma valor y se hace presente en la medida que los servicios que provee la plataforma de e-Gobierno se hacen más importantes y valiosos.

Aun antes de que logremos proveer acceso a Internet y a prestaciones de e-Gobierno a todos los ciudadanos de la región, debemos dar solución al gran problema de la seguridad de la información. Dado que la mayor parte de las prestaciones y transacciones de e-Gobierno no podrán concretarse con insuficientes niveles de seguridad de la información, es imprescindible diseñar -cada vez con mayor cuidado- los procesos, los flujos y la guarda de la información.

5.- ¿Cuán importante es la concienciación y la capacitación en materia de Seguridad de la Información en los gobiernos y en su relación con los ciudadanos?

En una respuesta anterior señalé la necesidad de que los ciudadanos tengan un entrenamiento básico, el cual debería

incluir -como mínimo- aspectos como: mantener actualizados los sistemas operativos y las aplicaciones, disponer de firewall activado y antivirus actualizado, adquirir licencias legítimas e ir a los sitios oficiales en caso de usar *software open source*.

Esas mismas políticas deberían ser seguidas por los administradores de instalaciones que ofrecen servicios de e-Gobierno. En ocasiones nos hemos encontrado con instalaciones que no cumplen con ningún *check list* de seguridad, con *passwords* por defecto, con políticas de seguridad anticuadas, etc. Es habitual encontrar al administrador de la solución muy enfocado con cumplir los tiempos de desarrollo y que la solución esté disponible con el deadline determinado por sus superiores, provocando descuidos o postergaciones en las revisiones de seguridad.

También el e-Gobierno debe acompañarse de marcos legales adecuados, como promover la protección de los datos personales, validar la firma electrónica y promover la transparencia, así como implantar mínimas políticas de seguridad informática al nivel de las organizaciones públicas. Todas estas actividades y un impulso sostenido contribuirán al mejor y más completo desarrollo del e-Gobierno.

PERFIL DE LOS ENTREVISTADOS

Belisario Contreras, CICTE-OEA

Administrador Asistente de Proyectos del Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA). Anteriormente se desempeñó como oficial de programas en el Young Americas Business Trust (YABT) de la OEA. Es Administrador de Empresas de la Universidad Francisco de Paula Santander (UFPS) y candidato a la Maestría de Estudios Latinoamericanos de la Escuela Edmund A. Walsh de Servicio Exterior de la Universidad de Georgetown

Mara Irene Misto Macías, Argentina

Desde 1985 se dedica a Tecnología de la Información tanto en el ámbito privado como el público. En el 2000 se especializa en Seguridad de la Información trabajando en la Secretaria de Hacienda del Ministerio de Economía y desde 2005 en el Banco Central de la República Argentina (BCRA), donde es responsable de promover el establecimiento de pautas, normas y estándares de seguridad respecto de la información sistematizada en la Institución, así como en las entidades que conforman el sistema financiero. Es Licenciada en Ciencias de la Computación de la Facultad de Ciencias Exactas de la Universidad de Buenos Aires, con postgrado de Especialización en Criptografía y Seguridad Teleinformática en el Instituto Superior del Ejército y de Desarrollo Gerencial en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Eduardo Wallier Vianna, Brasil

Responsable por la Coordinación General de Tratamiento de Incidentes de Seguridad en Redes de Computadores del Gobierno Federal de Brasil (CGTIR Gov) y miembro del Comité Gestor de Seguridad de la Información (CGSI). Es graduado en Tecnología de Procesamiento de Datos y en Aplicación y Planeamiento Militar. Se especializó en las áreas de Administración Pública, Gestión Estratégica de Sistemas de Información, Internet, Criptografía y Seguridad de Redes. Desde 1985, actúa en el sector público particularmente en el área de Seguridad de la Información. Se dedicó en la última década al estudio, enseñanza y aplicación de la gestión segura de las tecnologías de Información.

Eduardo Carozo Blumsztein, Uruguay

Gerente de Seguridad de la Información de la Administración Nacional de Telecomunicaciones (ANTEL) y Director Ejecutivo CSIRT-ANTEL, Uruguay, Integrante del Consejo de Seguridad Informática de la Presidencia de la República

Oriental del Uruguay, Integrante del Equipo Técnico de CERT.uy, Director del Proyecto AMPARO de LACNIC, Instructor Idel Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), Instructor de Análisis Organizacional del Banco Interamericano de Desarrollo (BID), Profesor de Proyectos de Inversión - Universidad de Montevideo, Gerente de Seguridad de la Información certificado por CIS-Austria. Es Ingeniero Civil Estructural de la Universidad de la República y cuenta con un. Máster en Gerencia de las Telecomunicaciones de la Universidad ORT, Uruguay.

SECCIÓN RIF GE

La Red Interamericana de Formación en Gobierno Electrónico (RIF-GE) del Colegio de las Américas (COLAM) de la Organización Universitaria Interamericana (OUI) fue creada en Washington DC en abril de 2004, en una reunión auspiciada por la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), con financiamiento del Instituto para la Conectividad de las Américas (ICA/IDRC). En dicha reunión, la creación de la RIF-GE fue decidida -por unanimidad- por los representantes de veintidós (22) instituciones de educación superior, organismos internacionales y regionales así como de organismos del sector público, provenientes de diecisiete (17) países de las nueve (9) regiones de la OUI.

En esta sección permanente nos proponemos difundir los avances en el conjunto de actividades de formación, investigación y servicios previstas en el Plan de Acción RIF-GE 2008-2011, que fuera concertado en el II Encuentro RIF-GE celebrado en Bogotá entre el 14 y el 16 de mayo de 2008.

Proyecto: "El ciudadano y el gobierno electrónico en las Américas": Llamado a propuestas de investigación

El 17 de septiembre de 2010, a las 17:00 horas (GMT – 4) se cerró el plazo para la recepción de propuestas de investigación correspondientes a la convocatoria "El Ciudadano y el Gobierno Electrónico en las Américas" organizada por el Centro Internacional de Investigaciones para el Desarrollo (IDRC) en colaboración con la Organización de los Estados Americanos (OEA), la Organización Universitaria Interamericana (OUI) y la Red de Gobierno Electrónico de América Latina y el Caribe (Red Gealc).

La selección de las propuestas está a cargo de un comité de expertos evaluadores, cuya composición se dará a conocer junto con el dictamen, el cual evaluará las propuestas con base en sus méritos técnicos y su potencial de aporte al desarrollo del e-Gobierno en la región de LAC. Los procesos de selección no estarán sujetos a reclamo ni apelación alguna.

Propuestas de investigación recibidas

Se recibieron cientouna (101) propuestas de investigación, enunciándose seguidamente -por orden alfabético de país y por orden de recepción- el/los países comprendidos, los títulos y las instituciones coordinadoras de cada propuesta.

1. Argentina, México: Desafíos y oportunidades del uso de las TIC en los gobiernos locales. Fundación Educativa San Andrés

2. Argentina, Brasil, Chile: Banco de datos ciclos de consagración normativa para la protección de grupos vulnerables en AL. Universidad de la Frontera

3. Argentina, Chile: Internet, Ciudadanía y Capital Social: construyendo gobierno electrónico local en comunidades rurales con un enfoque participativo. Centro de Investigación Sociedad y Políticas Públicas de la Universidad de los Lagos, Chile

4. Argentina: Gobierno Electrónico, ciudadanía y redes de conocimiento. Consejo Federal de Inversiones, Argentina

5. Argentina: Plataforma de Participación Ciudadana para el Estado de la Provincia de Santa Fe. Administración Provincial de Impuestos (API)

6. Argentina: Investigación sobre la implementación de civismo digital. Fundación TESA

7. Argentina: El Gobierno Electrónico en la Era de las Redes Sociales: Mejores prácticas de Comunicación de programas de Gobierno Electrónico a través de redes sociales. The Graduate School of Political Management at the George Washington University

8. Argentina: La información en la vida social: Sistema de aprendizaje cooperativo con información gubernamental autóctona. Universidad de la Matanza

9. Argentina: e-Gobierno y jóvenes: construyendo nuevas formas de participación. Instituto de Investigación en Medios

10. Argentina - Uruguay, Chile, Colombia, Paraguay El ciudadano y el gobierno abierto en América del Sur (CIGASUR). Fundación Gestión y Desarrollo

11. Argentina: Observatorio turístico en línea para el destino Villa Pehuenia. Facultad de Turismo, Universidad Nacional del Comahue

12. Argentina: Pami Integra: Las TIC como herramienta para una Argentina con Mayores Integrados. UTN. Universidad Tecnológica Nacional. Facultad Regional Mendoza. Secretaría de Extensión a través del Laboratorio de Gobierno Electrónico

13. Argentina: Las TIC como herramientas para una Argentina con Mayores Integrados. Universidad de Mendoza

14. Bolivia: Sistema de Información para integrar a los ciudadanos en la Gestión del Gobierno Municipal de la Ciudad de Cochabamba en Bolivia. Vox Terra

15. Bolivia, Colombia, Ecuador, El Salvador, Guatemala, Argentina y México: Transparencia pública y acceso a la información en entornos en línea en Latinoamérica. ONG Derechos Digitales

16. Brasil,- Argentina: Portais de Serviços Públicos e de Informação ao Cidadão: uma descrição do usuário. PUCPR Pontifícia Universidade Católica do Paraná

17. Brasil: Políticas de Governo Eletrônico em estados da Federação Brasileira: uma contribuição para análise segundo a perspectiva institucional. Fundação João Pinheiro

18. Brasil, Chile, El Salvador: Red latinoamericana de e-Gobierno y participación ciudadana. Universidad de Brasilia

19. Brasil: O cidadão em tela: ouvidoria municipal como instrumento de e-government. Universidade Federal da Bahia. Escola de Administração, através da Fundação Escola de Administração.

20. Brasil: O Governo Eletrônico na Bacia do Jacuípe, no Semi-árido Nordestino. FUNDAL – Fundação Antonio Almeida e Silva

21. Brasil: Avaliacao do nivel web dos municipios paulistas. FDTE

22.Brasil: e-Participacion como soporte de políticas. Fundación Jose Arthur Boiteux

23. Brasil: e-Parlamento. FUNDEP

24. Brasil: Redes sociales y e-Voting. I3G

25. Brasil: e-Participacion municipal. Universidad de Ceara

26. Brasil: Orçamento participativo digital (OPD): estratégias para aumento da participação cidadãna na América Latina. Instituto de Estudos, Formação e Assessoria em Políticas Sociais (Instituto Pólis)

27. Brasil: Utilização de serviços e-Gov pelo cidadão: uma análise dos fatores que influenciam em sua adoção. Universidade Federal do Rio Grande do Norte – UFRN

28. Brasil: Implantação de plataforma eletrônica de resgate e monitoramento da vóz pública: projeto piloto: painel de opinião popular / pop São Paulo Zona Sul. Centro de Estudos em Administração Pública e Governo da Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas

29. Brasil: Implantação de plataforma eletrônica de controle social de políticas públicas:- projeto piloto: observatório dos recursos do pac na Região dos Mananciais de São Paulo. Centro de Estudos em Administração Pública e Governo da Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas

30. Chile: Sistema de Buenas Prácticas en Gobierno Electrónico y Participación Ciudadana para América Latina y el Caribe: Observatorio Latinoamericano de Gobierno Electrónico y Participación Ciudadana (OLGEPAC). Instituto de Asuntos Públicos (INAP) – Universidad de Chile

31. Chile: Participación ciudadana en la implementación de salud electrónica para la reconstrucción sanitaria pública en la zona de catástrofe en Chile. Universidad de Concepción

32. Chile: Conductas de la población chilena en torno al uso del e-Gobierno. Universidad de Valparaíso

33. Chile: “Factores Técnicos y Económicos que Facilitan o Inhiben la Implementación de un Gobierno Abierto en la Región. Universidad Técnica Federico Santa María (Centro de Gobierno Electrónico)

34. Chile: Modelo para Diseñar Comunidades de Conocimiento en el Sector Agrícola. Universidad Técnica Federico Santa María (Centro de Gobierno Electrónico)

35. Colombia : Diseño del contenido básico y estrategia para la creación del "Portal de la Justicia en Colombia" de orientación al ciudadano. Corporación Excelencia en la Justicia

36. Colombia: Diseño de un punto neutro en los juzgados civiles de Bogotá. Corporación Excelencia en la Justicia

37. Colombia: Análisis de las relaciones y articulaciones entre la estrategia de gobierno en línea y Compartel. Corporación Univer. Minuto de Dios

38. Colombia : La vanguardia del gobierno en línea colombiano en pequeños municipios: red de experiencias significativas y su aplicación en la edición 2012 del manual de gobierno en línea. Fundación Incubadora Colombiana de Empresas (FICE)

39. Colombia: Riesgos de exclusión del ciudadano en la gestión del e-Gobierno municipal. Fundación Ortega y Gasset

40. Colombia: Proyecto Exclusión y Juventud. Universidad del SINU

41. Colombia: Estrategias para construir un modelo de gobierno electrónico en el municipio de Tunja. Incubadora de Empresas del Oriente, Incubar Boyacá

42. Colombia: La participación ciudadana a través del e-Government: Un estudio comparativo de los casos de Bogotá y San Juan de Pasto. Universidad del Rosario. Facultad de Ciencia Política y Gobierno

43. Colombia, Brasil: El ciudadano y la sociedad civil en procesos de gobernanza en red en áreas metropolitanas de América-Latina. Universidad Piloto de Colombia.

44. Colombia: La información del portal web del Sistema de Información Ambiental de Colombia (SIAC) como herramienta estratégica orientada hacia la participación de las y los ciudadanos en la gestión ambiental. Ministerio de Ambiente, Vivienda y Desarrollo Territorial (MAVDT)

45. Colombia : La comunidad ciudadana como gestora y diligenciadora de su propia información: el poder ciudadano para interactuar con el e-Gobierno. Escuela Superior de Administración Pública: ESAP. Boyacá y Casanare

46. Colombia : Identificación de las restricciones para la participación ciudadana en la planeación, ejecución, seguimiento y evaluación de la inversión pública en Bogotá Distrito Capital de Colombia como estudio de caso a a través del e-Gobierno. Universidad Nacional de Colombia

47. Colombia: Información para la Competitividad y Desarrollo Económico y Empresarial de Todos los Cundinamarqueses. Universidad EAN

48. Colombia: Lineamientos para la implementación de la litigación online en Colombia y diseño de una prueba piloto para su utilización en el trámite de la acción de tutela. Corporación Excelencia en la Justicia

49. Colombia: Tradición y escenarios en el municipio de Duitama y su influencia en la participación ciudadana y la disposición para la tele-democracia. Universidad Pedagógica y Tecnológica de Colombia

50. Colombia: El e-Gobierno, cultura del cambio y apropiación ciudadana para la gobernabilidad. Universidad Libre

51. Costa Rica: Aduanas costarricenses. Universidad de Costa Rica

52. Ecuador, Bolivia: Participación ciudadana en el gobierno electrónico al nivel local e intermedio y la sociedad civil en Ecuador y Bolivia. CEDIME

53. Ecuador: Red de intérpretes judiciales interculturales bilingües y relacionamiento de los sistemas de justicia ordinaria e indígena del Ecuador. Centro de Investigación de la Comunicación del Ecuador

54. El Salvador: Diagnostico y propuesta de plan de acción e-Gobes. Escuela Superior de Economía y Negocios

55. El Salvador: La participación ciudadana desde los portales web de las cabeceras departamentales de El Salvador. Asociación Conexión al Desarrollo de El Salvador

56. El Salvador: Gobierno electrónico en El Salvador: ¿cómo incluir a los jóvenes y las mujeres en la ciudadanía digital? Universidad Centroamericana José Simeón Cañas

57. México, Costa Rica: Modelo para incrementar la participación ciudadana en la gestión del e-Gobierno en el Estado de Colima México y la Municipalidad de San José Costa Rica. Universidad Colima

58. México. Desarrollo del GEMUS (Gobierno electrónico del Municipio de Solidaridad). Colegio de Ingenieros Civiles del Municipio de Solidaridad A.C.

59. México: TIC, profesionalización de servidores públicos y mejora de procesos. Dirección General de Innovación Tecnológica. Dirección General de Innovación Tecnológica

60. México: Registro Electrónico de Infracciones de Tránsito. Dirección General de Innovación Tecnológica. Dirección General de Innovación Tecnológica

61. México: Telecentros digitales como nexo entre e-Gobierno y comunidades marginadas. Universidad de Guadalajara

62. México: Uso de las TIC en Salud para el control y prevención de la Retinopatía Diabética, en comunidades aisladas del Estado de Veracruz, México. Instituto de Salud Pública de la Universidad Veracruzana

63. México, Perú, Chile: El diseño de un marco de referencia y de trabajo para evaluar la sustentabilidad de las soluciones de e-Gobierno y una metodología para el desarrollo de iniciativas centradas en el ciudadano, en ámbitos locales y regionales de México, Chile y Perú. Universidad de Guadalajara

64. México, El Salvador, Chile: Gobierno Electrónico en municipios de México, El Salvador y Chile: Diagnóstico y oportunidades. Centro de Sistemas Públicos

65. Nicaragua: Marco Conceptual para una Administración Municipal Contemporánea Apoyada en una Arquitectura Digital. UAM

66. Venezuela, Argentina, Chile, Brasil, Uruguay, Bolivia, Perú, Colombia, Guatemala, Nicaragua, México, República Dominicana: Ruta hacia la democracia digital personalizada en municipios de Latinoamérica. Transparencia Venezuela

67. Panamá: Si denuncias me ayudas. Instituto Panameño de Derecho de Consumidores y Usuarios

68. Paraguay: Ciudadanía y e-Gobierno. FUNDAINGE

69. Perú: Aporte de las tecnologías de información para la mejora de los procesos internos y provisión de los servicios en las municipalidades: estudio de caso de la Costa y Sierra Peruana. Centro de Educación y Comunicación Guaman Poma de Ayala

70. Perú: Sistema descentralizado de información laboral. Instituto Cuanto

71. Perú: Sistema Integrado de información educativa. Instituto Cuanto

72. Perú: Herramientas de e-Gobierno que incrementen la Participación Vecinal. Municipalidad de Miraflores

73. Perú: Perú e-gov. ONG Alfa-Redi

74. Perú: e-Gobierno. Sase Consultores S.A.C.

75. Perú: Ciudadanos diversos y gobierno electrónico: Análisis de las posibilidades de implementación y fortalecimiento de las estrategias de gobernabilidad vía uso de TIC en contextos locales diferentes. Instituto de Estudios Peruanos

76. Perú: e-Nacimientos en el Perú. Universidad Tecnológica del Perú

77. Perú. e-Ubicación. Universidad Tecnológica del Perú

78. Perú: e-Cultura. Universidad de San Martin de Porres

79. Perú: Sistema on-line para la recaudación tributaria municipal de los ciudadanos y pequeñas y medianas empresas (Pymes). Institute for Development

80. Perú: Usabilidad en Portales Ciudadanos Latinoamericanos: Un análisis a profundidad. Governa Estudios

81. Perú: Definición de atributos que inciden en el mayor uso de los servicios en línea. Governa Estudios}

82. Perú: Gobierno electrónico para el fortalecimiento del proceso de reparación a las víctimas de la violencia política en el Perú. Instituto de Estudios Peruanos

83. Perú: Estado del arte del m-Gobierno en América Latina y el Caribe: buenas prácticas y análisis del marco normativo. Governa Estudios

84. Perú: Gobierno Abierto: propuesta de un marco metodológico peruano. Caritas Arquidiocesana del Cusco

85. Perú: Comunidad virtual: ciudadanía y votación electrónica en el Perú a partir de la experiencia de América Latina. Oficina Nacional de Procesos Electorales

86. Perú: Desarrollo del Modelo Metodológico para la Inclusión de los Ciudadanos en el sistema de Administración Pública mediante el uso de Aplicaciones de Gobierno Electrónico en la Provincia de Cangallo. Universidad ESAN

87. Perú: Desarrollo del Modelo Metodológico para la Inclusión de los Ciudadanos en el sistema de Administración Pública mediante el uso de Aplicaciones de Gobierno Electrónico en la Provincia de Rioja. Universidad ESAN

88. Perú: Desarrollo del Modelo Metodológico para la Inclusión de los Ciudadanos en el sistema de Administración Pública mediante el uso de Aplicaciones de Gobierno Electrónico en el Distrito de Villa María del Triunfo. Universidad ESAN

89. Perú: Estrategias para un modelo interactivo de Gobierno Electrónico ante la exclusión del ciudadano en la gestión pública del Gobierno Regional de Lambayeque . Universidad Católica Santo Toribio de Mogrovejo

90. Puerto Rico: La participación ciudadana a través del e-gobierno municipal: el caso de Puerto Rico. Universidad de Puerto Rico. Recinto de Río Piedras

91. Uruguay: Sistema de e-Gobierno para la Autoridad Reguladora Nacional en Radio Protección. ARNR MIEM

92. Uruguay: Argentina, Bolivia, Brasil, Chile, Colombia, Ecuador, Perú, Paraguay, Venezuela: El gobierno electrónico en América del Sur: Diagnóstico, perspectivas y desafíos desde la gobernabilidad electrónica-democrática. Observatorio de Estrategias de Comunicación del Sector Público - Universidad Católica del Uruguay

93. Uruguay: Realidad de la gobernabilidad en la Administración Pública Loca. Universidad Católica de Uruguay

94.Uruguay: Gobierno Abierto: una agenda posible. Fundación Ciudad de Montevideo

95. Uruguay: Generando redes de soporte: Las posibilidades del e-Gobierno para la integración, interacción y participación de los sectores vulnerables y excluidos. ObservaTIC

96. Venezuela, Argentina: m-Gobierno. Asociación de Investigadores Venezolanos de la Comunicación (InveCom)

97. Venezuela: Geoportal Chacao. Instituto de Protección Civil y Ambiente

98. Venezuela, Brasil, Colombia. Chile, Costa Rica, República Dominicana: Gobierno electrónico pro-emprendedores: estudio impacto y potencial acelerador del gobierno electrónico desde la perspectiva de los emprendedores en 6 municipios de América Latina. Transparencia Venezuela

99. Venezuela: Ruta hacia la Democracia Digital, en municipios de Latino América. Transparencia Venezuela

100. Venezuela: Del Municipio Digital al Municipio Abierto. Concejo Municipal de Chacao

101.- Ecuador: El ciudadano y el gobierno electrónico en las Américas. Facultad de Ciencias Económicas de la Universidad Central del Ecuador

(*) Las propuestas 66 y 101 quedaron registradas fuera de orden alfabético

PARA TENER EN CUENTA

1.- Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA)

Objetivo: Ayudar a los Estados Miembros en el establecimiento de un equipo nacional permanentemente activo (los 7 días las 24 horas) de "alerta, vigilancia y advertencia," conocidos como Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT), a través de la asistencia técnica y capacitación; fortalecer las capacidades del personal designado de los CSIRT en los Estados Miembros para cumplir eficazmente con los requerimientos de la "Estrategia Integral Interamericana para Combatir Amenazas a la Seguridad Cibernética"; y facilitar la creación y mantenimiento de una Red Hemisférica de CSIRT para promover el compartir información y mejores prácticas.

Descripción: Este programa se compone de tres proyectos: a) talleres subregionales y hemisféricos; b) misiones de asistencia técnica para fortalecer las capacidades nacionales en los CSIRT; y c) capacitación y apoyo a la Red Hemisférica de CSIRT establecida en el servidor seguro de la OEA. La Secretaría de CICTE es una de las tres entidades de la OEA que tienen mandatos para asistir a los Estados Miembros en la implementación de la "Estrategia Integral Interamericana para Combatir Amenazas a la Seguridad Cibernética", adoptada por la Asamblea General de la OEA en 2004, y coordina sus actividades con el grupo de trabajo sobre crímenes cibernéticos de la Reunión de Ministros de Justicia de las Américas (REMJA) y el Comité Interamericano de Telecomunicaciones (CITEL) de la OEA.

Sitio web: http://www.cicte.oas.org/rev/es/programs/cybersecurity.asp

2.- Foro global de Equipos de Respuesta y Seguridad

FIRST (Forum of Incident Response and Security Teams) es un foro global de Equipos de Respuesta y Seguridad frente a Incidentes Informáticos (CSIRT) y es reconocido como líder en la materia. Reúne a una variedad de equipos de respuesta a incidentes en organizaciones gubernamentales, comerciales y educativas, exhibiendo en la actualidad más de 200 miembros en África, las Américas, Asia, Europa y Oceanía.

Apunta a fomentar la cooperación y la coordinación en la prevención y en la reacción rápida ante incidentes, así como a promover el intercambio y uso común de información entre los miembros y con la comunidad de seguridad. Ello permite a sus equipos miembros responder con mayor efectividad –reactiva y proactiva- a incidentes de seguridad.

Además de la red global de confianza en materia de respuesta a incidentes, FIRST provee servicios de valor agregado, tales como:

- Acceso a documentos actualizados de buenas prácticas
- Coloquios técnicos para expertos en seguridad
- Formación con intervención práctica
- Conferencia anual de respuesta a incidentes
- Publicaciones y servicios web
- Grupos de interés
- Programa Ejecutivo (CEP)

Sitio Web: http://www.first.org/

3.- Reunión de investigadores, fiscales y expertos gubernamentales contra el delito cibernético de Sudamérica

Investigadores, fiscales y funcionarios responsables de la asistencia internacional mutua de Argentina, Bolivia, Colombia, Ecuador, Paraguay, Perú y Uruguay, se reunieron en Lima, Perú, en el marco de un taller regional de capacitación celebrado entre los días 31 de agosto, 1 y 2 de septiembre de 2010, para analizar las actividades delictivas en que se utiliza el Internet, las tecnologías utilizadas por los delincuentes y las herramientas que ayudan a las agencias policiales a investigar y procesar a las personas que cometen estos delitos.

Este taller regional de capacitación en investigación de delitos por Internet a gran escala, desarrollado en cumplimiento de una de las recomendaciones adoptadas durante la VI Reunión del Grupo de Trabajo en Delito Cibernético del proceso de Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), se realizó gracias al auspicio del Departamento de Justicia de Estados Unidos, el Ministerio de Relaciones Exteriores del Perú, y la Secretaría General de la OEA a través del Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos.

Los ponentes del taller centraron sus exposiciones principalmente en los usos, tendencias y nuevas formas de delincuencia a través del Internet, en nuevas técnicas de investigación basadas en la informática forense, en aspectos jurídicos relativos a las pruebas electrónicas y en la importancia de la cooperación técnica y la asistencia recíproca internacional. El Director del Departamento de Cooperación Jurídica de la OEA, Dr. Jorge García González, realizó una presentación sobre los nuevos desarrollos e información contenidos en el Portal Interamericano de Cooperación en materia de Delito Cibernético como una herramienta útil para la cooperación y el intercambio de información entre los Estados miembros en el combate al delito cibernético, así como la utilidad de cada uno de los componentes que integran la Red en Materia Penal de la OEA para fortalecer la cooperación jurídica y judicial en la región.

Este taller en Lima es parte de un programa de cooperación auspiciado por el Departamento de Justicia del Gobierno de EE.UU. y por la Secretaría General de la OEA, en cuyo desarrollo se han organizado -durante los últimos dos años- encuentros en la materia a nivel subregional, en Trinidad y Tobago, Colombia, Chile, Panamá, Paraguay y México, los cuales serán continuados para los países del Caribe.

Para mayor información sobre estos talleres y otras acciones de la OEA para apoyar el combate contra el delito cibernético, consulte el "Portal Interamericano de Cooperación en materia de Delito Cibernético" Sitio web: http://www.oas.org/juridico/spanish/cybersp.htm

Fuente: OEA. Departamento de Cooperación Jurídica, Washington D.C.

4.- EE.UU.: Documento sobre Ciber-Seguridad

Institute for Information Infrastructure Protection (I3P): National Cyber Security Research and Development Challenges: Related to Economics, Physical Infrastructure and Human Behavior: An Industry, Academic and Government Perspective: A report to the Chairman and Ranking Member of the US Senate Committee on Homeland Security and Governmental Affairs, 2009

En el documento se señala que, frente a los desafíos presentes y previsibles, la ciber-seguridad debe ser adoptada como una prioridad nacional. Los sistemas que controlan gran parte de la infraestructura física de la nación –telecomunicaciones, energía, combustibles, agua- están cada vez más conectados con Internet y por tanto son vulnerables a nuevos tipos de amenazas no previsibles. Por su parte, los negocios, las cadenas de suministro y las instituciones financieras dependen significativamente de TIC que actualmente no reúnen suficiente confiabilidad ni seguridad. Las pérdidas económicas atribuidas a ataques TIC están alcanzando magnitudes que podrían afectar la seguridad económica de E.E.U.U.

Los participantes identificaron la necesidad de una agenda de investigación y desarrollo que: 1) focalice los impedimentos de mercado y regulatorios para una mejor ciber-seguridad, 2) asegure que la seguridad se construya dentro de los productos y procesos, y 3) desarrolle doctrinas nacionales e internacionales para la seguridad de información. Se identificaron tres estrategias de investigación y desarrollo que deben ser apoyadas por el gobierno: 1) asegurar la confidencialidad, integridad y disponibilidad de los datos en tiempo real generados por los sistemas de control de procesos, 2) procurar trazabilidad de los datos de entrada y de componentes físicos para ponderar su fiabilidad, y 3) desarrollar métricas para la seguridad.

Se coincidió en que la conducta humana es quizás la dimensión más desafiante y vulnerable entre las áreas consideradas, siendo las personas el eslabón más débil de la cadena de seguridad. La seguridad eficaz depende no sólo de la tecnología, sino fundamentalmente de los empleados, los aliados comerciales, los clientes y de otros usuarios de sistemas y redes de información.

Se concluyó con las siguientes prioridades de investigación y desarrollo: 1) aplicar protocolos fundados en las ciencias sociales para desarrollar una cultura efectiva de seguridad, 2) promover la creación e implementación de estrategias basadas en la motivación para prevenir y remediar el error humano inducido (uso erróneo y uso malicioso), 3) diseñar tecnologías de seguridad basadas en principios de efectiva interacción humana-computador para maximizar el cumplimiento del usuario, y 4) diseñar planes de estudios y programas de extensión para la generación K, de manera que la futura fuerza de trabajo tenga conciencia y respeto por la seguridad.

Incluye recomendaciones para el avance en la ciber-seguridad durante los próximos diez años, reconociendo cuatro áreas de necesidad: 1) Acercamiento coordinado y colaborativo entre el sector industrial, el académico y el gubernamental, 2) Desarrollo de herramientas de medición (métricas) de la seguridad y de sus consecuencias, 3) Creación de un marco legal y de política eficaz para la seguridad, y 4) Tratamiento de la dimensión humana de la seguridad.

Texto completo en pdf:
http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf
http://www.thei3p.org/news/senate_report.html
(Reseñó: J.L. Tesoro)

5.- EE.UU.: National Security Council: NSC Home Cybersecurity: The Comprehensive National Cybersecurity Initiative

El presidente Obama ha identificado a la ciber-seguridad como uno de los mayores desafíos –en términos económicos y de seguridad nacional- que enfrenta EE.UU. Poco después de su asunción, ordenó un estudio completo de los esfuerzos federales para defender la infraestructura de información y comunicaciones, así como el desarrollo de una perspectiva integrada para asegurar la integridad de la infraestructura digital de EE.UU.

Se instruyó al Coordinador de Ciber-seguridad del Poder Ejecutivo para: a) trabajar con distintos actores claves en la materia, incluyendo gobiernos estatales y locales, así como al sector privado, para asegurar una respuesta organizada y unificada a los incidentes previsibles, b) consolidar asociaciones público/privadas para hallar soluciones tecnológicas que aseguren la seguridad y prosperidad de E.E.U.U., c) invertir en investigación y desarrollo "de punta" para generar la innovación necesaria para enfrentar los desafíos digitales; y d) comenzar una campaña para promover conciencia de ciber-seguridad, así como la formación digital en todos los niveles para construir la fuerza de trabajo digital del siglo XXI.

Las actividades para ejecutar las recomendaciones del *Cyberspace Policy Review* se construyeron sobre la *Comprehensive National Cybersecurity Initiative* (CNCI) puesta en marcha por el ex presidente Bush en la Directiva Presidencial 23 (NSPD-54/HSPD-23) en enero de 2008.

El presidente Obama determinó que la CNCI y sus actividades asociadas deben evolucionar para constituirse en elementos claves de una estrategia nacional amplia y actualizada de ciber-seguridad.
La CNCI consiste en un conjunto de iniciativas interrelacionadas con los siguientes objetivos dirigidos a garantizar la seguridad de EE.UU. en el ciberespacio:

- Establecer una línea frontal de defensa contra amenazas actuales inmediatas mediante la creación o mejora de la ponderación situacional compartida de las vulnerabilidades, amenazas y eventos dentro del Gobierno Federal y -en última instancia- con gobiernos estatales, locales, tribales y con los aliados del sector privado, así como la capacidad de actuar rápidamente para reducir las vulnerabilidades actuales y para prevenir intrusiones.

- Construir una defensa efectiva contra todo el espectro de amenazas mediante el aumento de capacidades de contrainteligencia y el aumento de la seguridad en la cadena de suministro de tecnologías claves de información.

- Ampliar el entorno de la ciber-seguridad para el futuro, expandiendo la ciber-educación; coordinando y reorientando los esfuerzos de investigación y desarrollo a través del Gobierno Federal, así como definiendo y desarrollando estrategias para disuadir la actividad hostil o malévola en el ciber-espacio.

En la construcción de los planes para la CNCI, pronto se percibió que dichos objetivos no podrían alcanzarse si no se consolidaban simultáneamente ciertas capacidades estratégicas fundacionales claves dentro del Gobierno Federal. Por tanto, la CNCI contempla asignaciones para exigir el cumplimiento (*enforcement*) de las leyes federales, la inteligencia, y las comunidades de defensa para mejorar el ejercicio de funciones claves como la investigación penal; la recolección, procesamiento y análisis para la inteligencia; y el aseguramiento de información crítica para los esfuerzos nacionales de ciber-seguridad.

La CNCI fue desarrollada con gran atención a la protección de las libertades civiles y de los derechos a la privacidad, en estrecha consulta con expertos en privacidad del gobierno. Por otra parte, de acuerdo con el propósito declarado del presidente Obama de hacer de la transparencia una piedra basal de su gestión, la *Cyberspace Policy Review* identificó al uso común de información compartida como un componente clave de la ciber-seguridad efectiva.

La CNCI fue desarrollada con gran atención a la protección de las libertades civiles y de los derechos a la privacidad, en estrecha consulta con expertos en privacidad del gobierno. Por otra parte, de acuerdo con el propósito declarado del presidente Obama de hacer de la transparencia una piedra basal de su gestión, la *Cyberspace Policy Review* identificó al uso común de información compartida como un componente clave de la ciber-seguridad efectiva.

Para mejorar la comprensión pública de los esfuerzos federales, el Coordinador de Ciber-seguridad difundió una descripción sumaria de la CNCI, cuyas iniciativas básicas se enuncian seguidamente:

Iniciativa #1: Gestionar la Federal Enterprise Network como una única "*enterprise network*" mediante conexiones confiables.

Iniciativa #2. Desplegar un sistema de sensores de detección de intrusiones a través de la Federal Enterprise.

Iniciativa #3. Desplegar sistemas de prevención de intrusiones a través de la Federal Enterprise.

Iniciativa #4: Coordinar y reorientar las actividades de investigación y desarrollo en ciber-seguridad financiadas por el Gobierno.

Iniciativa #5: Conectar los actuales centros operativos de ciber-seguridad para mejorar la apreciación situacional y para compartir datos relativos a actividades maliciosas contra sistemas federales.

Iniciativa #6: Desarrollar e implementar un plan de ciber-contrainteligencia para todo el gobierno, para coordinar las actividades de todas las agencias federales para detectar, disuadir y mitigar las amenazas de ciber-inteligencia patrocinadas desde el exterior contra sistemas de información de E.E.U.U.

Iniciativa #7: Aumentar la seguridad de las redes clasificadas del Gobierno Federal.

Iniciativa #8: Expandir la ciber-educación para dotar a las personas de conocimiento, capacidades y habilidades para el uso seguro de las TIC.

Iniciativa #9: Definir, desarrollar y sustentar tecnologías, estrategias y programas de avanzada que puedan desplegarse en plazos de entre 5 y 10 años.

Iniciativa #10: Definir y desarrollar estrategias y programas de ciber-defensa y disuasión de eventuales interferencias y ataques en el ciber-espacio mejorando capacidades de alarma y advertencia, articulando roles públicos y privados, alianzas internacionales, y desarrollando respuestas apropiadas

Iniciativa #11: Desarrollar una perspectiva multi-dimensional para la gestión estratégica e integral de riesgos en la cadena global de suministro de TIC durante todo el ciclo vital de productos, sistemas y servicios.

Iniciativa #12. Definir el rol federal para extender la ciber-seguridad hacia ámbitos críticos de la infraestructura que sustenta la operación de sistemas y de las redes de información vulnerables a ciber-amenazas maliciosas.

Texto completo: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
(Reseñó: J.L. Tesoro)

NOTICIAS

1.- Próximos Cursos OEA sobre e-Gobierno

La Organización de los Estados Americanos (OEA) convoca al siguiente curso:

Modernización de la Gestión Catastral
Fechas de inicio y de finalización: 18 de octubre al 3 de diciembre de 2010.
Duración del curso: Siete (7) semanas (115 horas)

Idioma: El curso será dictado en español.

Información e inscripción:
http://portal.oas.org/LinkClick.aspx?fileticket=ebWJ9c%2b%2foUc%3d&tabid=1790

ENLACES

Enlaces sugeridos a los interesados en la temática “e-Gobierno y Seguridad de la Información”

Alemania. Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/cln_174/DE/Home/home_node.html

Alemania. Centro de Seguridad Informática
https://www.cert.dfn.de/

Alemania. Federal Office for Information Security
https://www.bsi.bund.de/cln_174/EN/Home/home_node.html

Argentina. Jefatura de Gabinete de Ministros. Secretaría de la Gestión Pública. Subsecretaría de Tecnologías de Gestión: Coordinación de Emergencias en Redes Teleinformáticas
http://www.arcert.gov.ar/

Argentina. Jefatura de Gabinete de Ministros. Secretaría de la Gestión Pública. Subsecretaría de Tecnologías de Gestión. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional
http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf

Argentina. Jefatura de Gabinete de Ministros. Secretaría de la Gestión Pública. Subsecretaría de Tecnologías de Gestión: Oficina Nacional de Tecnologías de Información (ONTI)
http://www.sgp.gov.ar/contenidos/onti/onti.html

Asociación Española para el Fomento de la Seguridad de la Información (España)
https://www.ismsforum.es/home/index.php

Australia. Australian Computer Emergency Response Team
http://www.auscert.org.au/

Brasil: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
http://www.cert.br/

Canadá: Personal Information Protection and Electronic Documents Act
http://laws.justice.gc.ca/eng/P-8.6/index.html

Canadá: Public Safety Canadá
http://www.publicsafety.gc.ca/

Canadá: Security of Information Act
http://laws.justice.gc.ca/en/O-5/index.html

Carnegie Mellon University. Software Engineering Institute (EE.UU., USA): CERT Coordination Center
http://www.cert.org/
Center for Strategic and International Studies (CSIS) (EE.UU., USA): Securing Cyberspace for the 44th Presidency. Center for Strategic and International Study's (CSIS's). Commission on Cybersecurity for the 44 th Presidency
http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

Chile. Agenda Digital: Norma Técnica sobre Seguridad y Confidencialidad del Documento Electrónico. Chile. Junio 2004
http://www.agendadigital.cl/files/decreto_83.pdf

Chile. Servicio Médico Legal. Manual de Procedimientos del Departamento de Informática
http://www.sml.cl/portal/pdfs/manualInformatico.pdf

China. National Computer Network Emergency Response Technical Team
http://www.cert.org.cn/english_web/index.htm

COBIT (Control Objectives for Information and related Technology)
Conjunto de mejores prácticas para el manejo de información. Asociación para la Auditoría y Control de Sistemas de Información (ISACA -Information Systems Audit and Control Association) e Instituto de Administración de las Tecnologías de la Información (ITGI - IT Governance Institute
http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
http://www.itil.org/en/vomkennen/cobit/index.php

Comisión Europea: Directiva 2006/24/Ce del Parlamento Europeo y del Consejo de 15 de marzo de 2006 Conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF

Comisión Europea: Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. Privacidad
Mònica Vilasau Solana (UOC)
http://www.uoc.edu/idp/3/dt/esp/vilasau.pdf

Comisión Europea: European Comission. European eGovernment Services
http://ec.europa.eu/idabc/en/home

Comisión Europea: European Comission. Information Society and Media
http://ec.europa.eu/dgs/information_society/index_en.htm

Comisión Europea: European Network and Information Security Agency
http://www.enisa.europa.eu/

Corea: CERT
http://www.krcert.or.kr/

CriptoRed. Red Tematica de Criptografia y Seguridad de la Información
http://www.criptored.upm.es/

CSSIA. Center for System Security and Information Assurance. Cyber Defense Training Center (EE.UU, USA)
http://www.cssia.org/

Dinamarca. National IT and Telecom Agency
http://en.itst.dk/

EE.UU. (USA):.Computer Crime & Intellectual Property Section
http://www.justice.gov/criminal/cybercrime/

EE.UU. (USA). United States Computer Emergency Readiness Team
http://www.us-cert.gov/federal/

EE.UU. (USA). GFirst. Government Forum of Incident Response and Security Teams
http://www.us-cert.gov/GFIRST/presentations.html

EE.UU. (USA). Homeland Security: Office of Infrastructure Protection. National Programs and Protection Directorate.
http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm
http://www.dhs.gov/xabout/compliance/

EE.UU. (USA). National Coordinating Center for Telecommunications (NCC)
http://www.ncs.gov/ncc/

EE.UU. (USA). National Institute of Standards and Technology. Information Technology Laboratory Computer Security Division. Computer Security Resource Center
http://csrc.nist.gov/

EE.UU. (USA): Securing Cyberspace for the 44th Presidency
A Report of the CSIS Commission on Cybersecurity for the 44th Presidency
http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

EE.UU. (USA):.United States Computer Emergency Readiness Team. Federal Incident Reporting Guidelines.
http://www.us-cert.gov/federal/reportingRequirements.html

Entrevista a Carlos Sáiz por los Informativos de TVE 1 en materia de Ciberdefensa de Estado
http://legal4.ecija.com/documentos/Gabinete%20de%20Comunicacion/Entrevista_Carlos_Saiz_por_los_informativos_de_TVE1.pdf
http://www.youtube.com/watch?v=rjz7s6_gv8o

EPIC. Electronic Privacy Information Center
http://epic.org/

España. Alcaldía de Pamplona. Manual para la administración del riesgo
http://pamplonita-nortedesantander.gov.co/apc-aa-files/666334303434643463386666623264 39/MCG__MA_01_MANUAL_PARA_LA_ADMINISTRACION_DE_RIESGOS.pdf

España: Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)
http://www.cnpic-es.es/cnpic/

España. Gobierno Vasco. Manual de Seguridad Aplicaciones de Tramitación Telemática (Platea). Departamento de Justicia y Administración Pública
http://www.belt.es/legislacion/vigente/Seg_inf/Seg_inf/estatal/210410-Manual-Seguridad.pdf

España. Grupo de Delitos Telemáticos de la Guardia Civil
http://www.facebook.com/GrupoDelitosTelematicos

España. Instituto Nacional de Tecnologías de la Comunicación (INTECO). Agencia Española de Protección de Datos Guía sobre seguridad y privacidad de la tecnología RFID
http://www.inteco.es/file/KUS8RlRmcqJe53XLtJgjzw

España. Instituto Nacional de Tecnologías de la Comunicación: (INTECO): Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online
http://www.inteco.es/file/vuiNP2GNuMinSjvyZnPW2w

España. Instituto Nacional de Tecnologías de la Comunicación: (INTECO): Estudio sobre la Seguridad de la Información y e-Confianza en el ámbito de las Entidades Locales
http://www.inteco.es/file/sQgQjLaGEUmFTm-Pnltwyg

España. Instituto Nacional de Tecnologías de la Comunicación: (INTECO): Estudio sobre la seguridad de los datos de carácter personal en el ámbito de las Entidades Locales españolas
http://www.inteco.es/file/_FdmOHcQW39sU91F5d6cwg

España. Instituto Nacional de Tecnologías de la Comunicación (INTECO): Guía legal sobre Protección de Datos de Carácter Personal
https://www.inteco.es/file/mJct2kagT45sU91F5d6cwg

España. Instituto Nacional de Tecnologías de la Comunicación (INTECO): Guía legal sobre Videovigilancia
http://www.inteco.es/file/13Fbv21hF4jRgUc_oY8_Xg

España. Instituto Nacional de Tecnologías de la Comunicación (INTECO): Guía sobre la respuesta jurídica a los ataques contra la Seguridad de la Información
http://www.inteco.es/file/ePXa1SmtJPgGEiZl7GiXgQ

España. Instituto Nacional de Tecnologías de la Comunicación: (INTECO):. Observatorio de Sociedad de la Información. Instituto Nacional de Tecnologías de la Comunicación (INTECO),
http://www.inteco.es

España. Ministerio de Administraciones Públicas. Consejo Superior de Administración Electrónica: Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la seguridad de la Tecnología de la Información
http://www.csae.map.es/csi/pg3433.htm

España. Ministerio de Administraciones Públicas. Consejo Superior de Administración Electrónica: Comunicación de la Comisión de las Comunidades Europeas sobre Seguridad de las redes y de la información: Propuesta para un enfoque político europeo (COM(2001) 298 final),
http://www.csae.map.es/csi/pdf/com2001_0298es01.pdf

España. Ministerio de Administraciones Públicas. Consejo Superior de Administración Electrónica: Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
http://www.csae.map.es/csi/pg3443.htm

España. Ministerio de Administraciones Públicas. Consejo Superior de Administración Electrónica: MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
http://www.csae.map.es/csi/pg5m20.htm

España. Ministerio de Administraciones Públicas. Consejo Superior de Administración Electrónica:: Ministerio de la Presidencia: Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
http://www.csae.map.es/csi/pdf/RD_3_2010_texto_consolidado.pdf

España. Ministerio de Administraciones Públicas. Consejo Superior de Administración Electrónica: Normalización en seguridad de las tecnologías de la información..
http://www.csae.map.es/csi/pg3441.htm

España. Ministerio de Administraciones Públicas. Guía de Autoevaluación para la Administración Pública: Modelo EFQM de Excelencia
http://www.aeval.es/comun/pdf/Guia_EFQM_corta_04_06.pdf

España: Primer Encuentro Internacional CIIP. Ciberseguridad y Protección de las Infraestructuras Críticas de Información
http://forumciip.cnpic-es.com/

FIRST: Forum of Incident Response and Security Teams
http://www.first.org/

Foro Meridian. Promoción de regulaciones específicas, relaciones y colaboración en el ámbito de las infraestructuras críticas de la información (ICI).
http://meridianprocess.org/

Francia. Agence nationale de la sécurité des systèmes d'information (ANSSI)
http://www.ssi.gouv.fr/

Francia. Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA)
http://www.certa.ssi.gouv.fr/

Francia. Club de la Sécurité de l'Information Français
https://www.clusif.asso.fr/index.asp

Francia: Mehari. Conjunto de herramientas y funcionalidades metodológicas para la gestión de la seguridad
https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduccion.pdf

Francia. Portail de la sécurité informatique
http://www.securite-informatique.gouv.fr/

Francia. Secrétariat Général de la Défense Nationale
http://www.sgdn.gouv.fr/

Guía para la Seguridad en áreas críticas de atención en Cloud Computing V2
http://www.ismsforum.es/img/a25/na235_GUIA_CSA_PARA_LA_SEGURIDAD_EN_AREAS_CRITICAS_DE_ATENCION_EN_CLOUD_COMPUTING_V2.pdf

Hong Kong. Computer Emergency Response Team Coordination Centre
http://www.hkcert.org/english/home.html

Information Technology Infrastructure Library (ITIL): Biblioteca de Infraestructura de Tecnologías de Información
http://www.itil-officialsite.com/home/home.asp
http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf

Inside Facebook security, and how to better protect your account
http://www.sophos.com/blogs/gc/g/2010/09/29/facebook-security-protect-account

ISAC: International: Information Sharing and Analysis Centers Council (ISAC Council)
http://www.isaccouncil.org

ISO: Norma ISO/IEC 27001:2005
Proporciona un modelo para implementar y administrar un sistema de gestión de seguridad de la Información (SGSI)
http://www.27000.org/

ISO: Norma. ISO 27001, ISO 27002 (ISO 17799) Community Forum
http://www.17799.com/
http://es.wikipedia.org/wiki/ISO/IEC_17799

ISO: Norma ISO/IEC 27002:2005: Directrices y principios generales para la puesta en marcha, implementación, mantenimiento y mejora de la gestión de la seguridad de la información
http://www.27000.org/

ISO: Norma ISO/IEC 27005:2008: Marco mínimo de trabajo y descripción de requerimientos para el proceso de evaluación de riesgos
http://www.27000.org/

ISO. Subcomité 27 del JTC 1 - IT Security techniques.
http://www.iso.org/iso/standards_development/technical_committees/other_bodies/iso_technical_committee.htm?commid=45306

ISO/IEC 20000. Gestión de servicios de TI
http://www.iso20000.ch/en/vomkennen/iso20000/index.php

Italia. UACI (Computer Crime Analysis Unit)
http://www.poliziadistato.it/articolo/986-Unita_di_analisi_sul_crimine_informatico_Computer_Crime_Analysis_Unit

Markle Foundation Task Force on National Security in the Information Age
http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php

México. Dirección General de Cómputo y de Tecnologías de Información y Comunicación. Subdirección de Seguridad de la Información/UNAM-CERT,.
http://www.seguridad.unam.mx/index.html

NATO: NATO Computer Incident Response Capability (NCIRC)
http://www.ncirc.nato.int/

Noruega: Norwegian National Security Authority
https://www.nsm.stat.no/Globale_funksjoner/Global-menu/In-English/

OCDE; Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad
http://www.csae.map.es/csi/pdf/ocde_directrices_esp.pdf

OEA: Aspectos Jurídicos de la Seguridad de la Información y las Comunicaciones:. Criptosistemas. José María Molina
http://www.oas.org/juridico/spanish/cyb_ecu_aspectos_juridicos.pdf

OEA: Comité Interamericano Contra el Terrorismo (CICTE)
http://www.cicte.oas.org/Rev/es/

OEA: Estados Unidos. Red 24/7 para Delitos de Alta Tecnología. Albert Rees. Sección Delitos Informáticos y Propiedad Intelectual . Departamento de Justicia de los Estados Unidos
http://www.oas.org/juridico/spanish/cyb20_network_sp.pdf

OEA: Portal Interamericano de Cooperación en materia de Delito Cibernético. OEA
http://www.oas.org/juridico/spanish/cybersp.htm

Países Bajos. NAVI - Nationaal Adviescentrum Vitale Infrastructuur
https://www.navi-online.nl/

Perú. División de Investigación de Delitos de Alta Tecnología
http://www.policiainformatica.gob.pe/

Perú. Autorizan ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010". RESOLUCIÓN MINISTERIAL N°187-2010-PCM
http://www.pcm.gob.pe/Transparencia/Resol_ministeriales/2010/RM-187-2010-PCM.pdf

Prácticas de Seguridad de la Información: Reflexiones en la Web 2.0. Jeimy J. Cano, Ph.D, CFE
http://www.acis.org.co/fileadmin/Revista_116/Uno.pdf

Primera Campaña contra el robo de identidad y el fraude on-line (España)
http://www.nomasfraude.com/spain/

Purdue University. The Center for Education and Research in Information Assurance and Security (CERIAS) (EE.UU., USA)
http://www.cerias.purdue.edu/

Purdue University. The Center for Education and Research in Information Assurance and Security (CERIAS) (EE.UU., USA): Developing a Risk Management System for Information Systems Security Incidents. Fariborz Farahmand. College of Computing. Georgia Institute of Technology
https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/Farahmand.pdf

Purdue University. The Center for Education and Research in Information Assurance and Security (CERIAS) (EE.UU., USA): Digital Government Security Infrastructure Design Challenges. James Joshi, Arif Ghafoor, Walid G. Aref, Eugene H. Spafford
http://www.cerias.purdue.edu/ssl/techreports-ssl/2001-31.pdf

Reino Unido: Centre for the Protection of National Infraestructure (CPNI)
http://www.cpni.gov.uk/

Security Management. Jacques A. Cazemier,Paul L. Overbeek,Louk M. C. Peters
http://books.google.es/books?id=1ANBY4CEQ0cC&dq=%22Central+Computer+and+Telecommunications+Agency%22&printsec=frontcover&source=bl&ots=xM-0sLCgVz&sig=dThX4iNDt6mWp6y5aEblxbrWGDY&hl=es&ei=S-jKSZ3wEczJtgfJ2anbCQ&sa=X&oi=book_result&resnum=5&ct=result#v=onepage&q=%22Central%20Computer%20and%20Telecommunications%20Agency%22&f=false

Seguridad de la Información en Latinoamérica. Jeimy J. Cano.
http://www.acis.org.co/fileadmin/Revista_110/05investigacion1.pdf

SocInfo: Documentación y seguridad electrónica. Revista Electrónica SocInfo
http://www.socinfo.info/seminarios/docu.htm

SocInfo: Planes de Seguridad y Protección de Datos en las Administraciones Públicas. Revista electrónica SOCINFO
http://www.socinfo.info/seminarios/datos.htm

SocInfo: Seguridad y Protección de Datos (II). Revista electrónica SOCINFO
http://www.socinfo.info/seminarios/datos2.htm

Taiwan Computer Emergency Response Team
http://www.cert.org.tw/eng/

Nota: Invitamos a todos los lectores a sugerirnos la inclusión de recursos y a avisarnos en caso de que alguno de los vínculos publicados se hallara dañado. Con esta colaboración podremos ofrecer un mejor material. Dirigir sus sugerencias y avisos a: Javier Sáenz Coré <jsaenzcore@gmail.com>

(*) El correcto funcionamiento de los URL indicados en cada una de las referencias de esta sección fue verificado entre los días 28 y 30/09/2010.