Seguridad de la Información en el Uruguay: Políticas de Estado en la Administración Pública

Esc. Ma. Claudia Pereiro Alonso[1]

Integrante de la Comisión de Derecho Informático de la Asociación de Escribano del Uruguay

Abstract: El presente trabajo parte de los conceptos de Gobierno Electrónico - Gobierno en Red y de la Seguridad Informática, para concluir en las políticas concretas que se han instrumentado para la Administración Pública en el Uruguay, en esa última materia. Incluye anexo con cronología de normativa nacional a partir de los años ochenta, su consolidación entre 2005 - 2010 y Organismos competentes.-

Palabras Clave: Seguridad, Información, Gobierno Electrónico, Sistemas de Gestión de Seguridad de la Información.

1 Gobierno Electrónico. Concepto.

Según El Banco Mundial (2003) el Gobierno Electrónico "se refiere al uso de tecnologías de información por parte de las agencias gubernamentales que tienen la habilidad de transformar las relaciones entre los ciudadanos, los negocios y otros brazos del gobierno"

La Comisión Europea para la información entiende que es "para la gente que esté en línea y no en fila". Reinermann (2001) dice que es la "transformación de instituciones públicas en el ciber-espacio, un área sin restricciones de espacio, tiempo o jerarquías". Y finalmente Di Maio (2002), a su vez, afirma que es la "transformación de relaciones internas y externas del sector público a través de operaciones realizadas por Internet y tecnologías de información para optimizar la entrega de servicios por parte del gobierno y la participación ciudadana". [2]

El Prof. Fernando Galindo afirma que se llama Gobierno Electrónico a las "relaciones establecidas entre ciudadanos y funcionarios o personal de las Administraciones Públicas utilizando las TIC". Electrónico significa el aprovechamiento de las Tecnologías de Información y Comunicación para aumentar la inclusión de amplios sectores que han estado al margen de la acción social del Estado. Las Tecnologías de Información no sólo pueden propiciar la transformación del Estado, maximizando la eficiencia de la Administración Pública, también son un mecanismo para aumentar la transparencia y garantizar la seguridad de la nación.

El Gobierno electrónico se puede definir como "las transacciones: procedimientos jurídicos realizados entre las Administraciones Públicas entre sí, o entre los ciudadanos o empresas y las Administraciones Públicas, utilizando como recurso complementario las

[1] Dirección Espinillo 1374, Montevideo, Uruguay, correo electrónico mcpereiro@gmail.com

[2] Banco Mundial (2003) en línea Septiembre 2005 http://www1.worldbank.org/publicsector/egov/definition.htm
Di Maio, A., Baum C., Keller B., Kreizman G., Pretali M and Seabrook D (2002) Framework for eGovernment Strategy Assessment" Gartner, Stanford, Connecticut USA

tecnologías de la información y la comunicación" (redes de banda ancha, Internet, telefonía móvil, etc.). El Gobierno Electrónico persigue incrementar la transparencia y eficiencia del sector público, proveer medios ágiles de información y comunicación para los ciudadanos, asegurando el desarrollo sostenible. Deber ser: oportuno: en relación al tiempo; idóneo: en relación a la adecuación; seguro; transparente: en cuanto a su eficiencia y eficacia, así como en el acceso a sus presupuestos y ejecuciones; debe garantizar la probidad y resultar ser satisfactorio al ciudadano.

La mayoría de los gobiernos han pasado por cuatro etapas principales: 1) creación de un portal informativo, o interacción con el ciudadano, 2) interacción bidireccional, 3) implantación de funcionalidades estructuradas que permitan a los ciudadanos realizar transacciones y 4) la instalación de un portal integrador Inter – organismos, que abarque todos los servicios posibles desde Internet. Esta evolución avanza hacia el Estado descentralizado en Internet, mediante la integración en las redes y en los servicios de comunicación electrónicas del conjunto de las Administraciones Publicas, cualquiera sea su jerarquía y posición Institucional. Tal intercomunicación apareja la necesidad de la adaptación de las soluciones normativas, la utilización de estándares internacionales y lo que se denomina convergencia de los Derechos Administrativos. [3]

2 Seguridad Informática. Concepto.

La *seguridad* es la cualidad de seguro, libre de riesgo, se aplica a mecanismos que precaven de fallas en el funcionamiento de algo. La seguridad es un valor al que se aspira, aun cuando se conoce que nunca nada será 100% seguro.

Por su parte la *seguridad jurídica*, alude a la certeza, el orden, la firmeza y la confianza en el ordenamiento en las relaciones jurídicas entre individuos y entre el individuo y la Administración. Es entonces, un principio general de Derecho, soporte primario y estructural del sistema jurídico, verdadero cimiento que sirve como criterio interpretativo, colmando vacíos normativos y constituye fuente de derecho. Plasmada en una ley, conforma el reconocimiento legal de los procedimientos que utiliza la seguridad informática, otorgándole la imperatividad natural de la misma.

En el Derecho Telemático el concepto de seguridad se potencia como un gran objetivo. Frente al uso de ordenadores en red y de Internet los problemas de seguridad pueden dividirse en básicamente cuatro áreas: el secreto, la validación de identificación, el no repudio y el control de integridad. Para atenderlas deben adoptarse medidas a nivel de hardware y de software.

La seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto. Otros autores la definen como la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

Enunciado: "La Seguridad de la información es el conjunto de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recursos humanos integrados para proveer toda la protección debida y requerida a la información y a los recursos informáticos de una empresa, institución o agencia gubernamental"[4]

---

[3] El E – procurement o el nuevo rostro de la contratación Administrativa. Dr. Carlos E Delpiazzo. Derecho Informático FCU Tomo III

[4] Escuela Colombiana de Ingeniería Julio Garavito, SYPI Semestre II 2005, Notas del profesor Fascículo No2, Ingeniero Jaime Hernando Rubio Rincón

En el respectivo prefacio de las "Directrices de la OCDE[5] para la Seguridad de Sistemas y Redes de Información. Hacia una cultura de seguridad."[6], se enfatiza en que la alta interconexión de los participantes mas allá de sus fronteras nacionales; el extendido uso de Internet, la que desempeña un papel fundamental en la forma en que las compañías realizan sus transacciones comerciales, los gobiernos desempeñan sus servicios a los ciudadanos y a las empresas, y los ciudadanos se comunican e intercambian información en manera individual; el numero y tipo de dispositivos que integran la infraestructura de acceso, traen como consecuencia un aumento de las vulnerabilidades. Esto hace surgir nuevos retos en materia de seguridad, por lo cual dichas directrices recomiendan tener una mayor conciencia y entendimiento de los aspectos de seguridad, así como la necesidad de desarrollar una "cultura de seguridad".

Las citadas directrices recomiendan nueve principios complementarios entre sí:

1. Concienciación: los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.
2. Responsabilidad: todos los participantes son responsables de la seguridad de los sistemas y redes de información
3. Respuesta: los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
4. Ética: los participantes deben respetar los intereses legítimos de terceros.
5. Democracia: la seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática
6. Evaluación del riesgo: los participantes deben llevar a cabo evaluaciones de riesgo.
7. Diseño y realización de la seguridad: los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.
8. Gestión de Seguridad: los participantes deben adoptar una visión integral de la administración de la seguridad
9. Reevaluación: los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, practicas, medidas y procedimientos de seguridad.

La seguridad de la Información, se resume, en cinco objetivos principales[7]:

Integridad: Hace alusión a la validez y consistencia de los elementos de información almacenados y procesados. Importante en sistemas descentralizados[8]. Garantiza que los datos

[5] Organización de Cooperación y Desarrollo Económico. (Organization for Economic Co-operation and Development)

[6] Adoptadas como Recomendación del Consejo de la OCDE en su 1037 sesión de 25 de julio de 2002

[7] Confidencialidad, Integridad y Disponibilidad, recogidos por el documento de Política de Seguridad de la Información para Organismos de la Administración Publica, confeccionado por AGESIC, ref. Pág. Web www.agesic.gub.uy

[8] Sistema Descentralizado: Un sistema se dice centralizado cuando tiene un núcleo que comanda a todos los demás, y estos dependen para su activación del primero, ya que por sí solos no son capaces de generar ningún proceso. Por el contrario descentralizado son aquellos donde el núcleo de comando y decisión está formado por varios subsistemas. En dicho caso el sistema no es tan dependiente, sino que puede llegar a contar con subsistemas que actúan de reserva y que sólo se ponen en funcionamiento cuando falla el sistema que debería actuar en dicho caso.

sean los que se supone que son. La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).
Confidencialidad: Hace alusión a la privacidad de información almacenada y procesada. Es de importancia en sistemas distribuidos[9]. Asegura que sólo los individuos autorizados tengan acceso a los recursos que se intercambian. Consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación
Disponibilidad: Hace alusión a la continuidad de acceso a los elementos de información almacenados y procesados y a garantizar el correcto funcionamiento de los sistemas de información. El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.
Evitar el rechazo: Garantizar de que no se pueda negar una operación realizada. Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada
Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos. La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización. Debe responder a: 1. Que es necesario proteger, 2. De que es necesario protegerlo y 3. Cuales van a ser las medidas físicas y lógicas que usará una la organización.

Por lo tanto, la Alta Dirección debe definir una política que refleje las líneas directrices de la Organización en materia de seguridad, aprobarla, y publicitarla a todos los involucrados.

Deben definirse claramente las necesidades de la Organización, a través de inventarios del sistema de información que recopile por ejemplo las personas, sus funciones, materiales, equipamiento, servicios, esquema de la red, infraestructura de comunicaciones, información delicada. Asimismo corresponde analizar riesgos y amenazas, estimar sus probabilidades y estudiar su impacto, definir las medidas de protección, y monitorear su cumplimiento. Abarca también definir claramente las responsabilidades de cada usuario y de cada área de trabajo, desde un punto de vista universal, ya que los problemas de seguridad no son exclusivamente técnicos.

3 Estándares

La información es un activo vital para el éxito y continuidad en el mercado de cualquier organización. El aseguramiento de dicha información es un objetivo de primer nivel para las mismas. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que este sometida

ISO/IEC 17799[10]

A los efectos de normalizar las practicas de las organizaciones, surge en el año 2000 la ISO 17799, cuyo objetivo es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una practica eficaz de la gestión de la seguridad. Norma no certificable, que recoge la relación de controles a aplicar o a evaluar para establecer

[9] Sistema Distribuidos: Sistemas cuyos componentes hardware y software, que están en ordenadores conectados en red, se comunican y coordinan sus acciones mediante el paso de mensajes, para el logro de un objetivo. Se establece la comunicación mediante un protocolo prefijado por un esquema cliente-servidor

[10] ISO (International Organization for Standardization)/IEC (International Electro technical Commission)

un Sistema de Gestión de la Seguridad de la información según la norma UNE 71502[11], si certificable. Dicha norma incluye diez dominios de control que cubren por completo la gestión de Seguridad de la Información: Política de Seguridad, Aspectos Organizativos para la seguridad, Clasificación y control de Activos, Seguridad ligada al personal, Seguridad Física y del entorno, gestión de comunicaciones y operaciones, Control de Accesos, Desarrollo y mantenimiento de sistemas, gestión de continuidad del negocio y Conformidad con la legislación.-

De estos diez dominios se derivan 36 objetivos de control, resultados esperados y 127 controles, practicas, procedimientos o mecanismos que reducen el nivel de riesgo.

ISO/IEC 27000

En el 2005 al tiempo de que se reviso y actualizo la norma 17799 es renombrada como ISO/IEC 27000 y su serie. Esta norma conforma un *conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información para cualquier tipo de organización pública o privada*. En un detalle somero de las mismas:

- **ISO/IEC 27000**: Fundamentos y vocabulario.
- **ISO/IEC 27001**: Norma que especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI). Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.
- **ISO/IEC 27002**: (previamente BS 7799 Parte 1 y la norma ISO/IEC 17799): Código de buenas prácticas para la gestión de Seguridad de la Información, describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

- **ISO/IEC 27003*:*** Directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Es el soporte de la norma ISO/IEC 27001. Describe el proceso de implementación del Sistema, prestando soporte en los siguientes puntos: aprobación de dirección y autorización para la realización del proyecto, definición del alcance, limites y fronteras, la evaluación de los riesgos y el plan del tratamiento de los mismos, el diseño del SGSI y la planificación del proyecto de implementación.[12]

[11] antecedentes: BS 7799 (1995) y BS 7799-2 (1998)

[12] **Estructura y contenido de la norma 27003:** hasta los títulos de segundo nivel: **1. Alcance; 2. Referencias normativas; 3. Términos y definiciones; 4. Estructura de esta norma internacional:** 4.1 Estructura general de las cláusulas, 4.2 Estructura general de una cláusula, 4.3 Diagramas**; 5. La obtención de autorización de la dirección para iniciar un proyecto de SGSI,** 5.1 Descripción general de aprobación de la gerencia de iniciar el proyecto SGSI, 5.2 Aclarar la organización prioridades para desarrollar un SGSI, 5.3 Definir el alcance preliminar SGSI, 5.4 Crear el caso de negocio y el plan de gestión de proyecto para su aprobación; **6 Definir el alcance SGSI**, **fronteras y política de SGSI,** 6.1 Información general sobre la definición de alcance SGSI, fronteras y la política de SGSI, 6.2 Definir el alcance y los límites de la organización, 6.3 Definir la información y la comunicación (TIC) alcance y sus límites, 6.4 Definir el alcance y los límites físicos, 6.5 Integrar cada ámbito y los límites para obtener el alcance y los límites SGSI, 6.6 Desarrollar la política de SGSI y obtener la aprobación de la gestión; **7 La realización de los requisitos de información de análisis de seguridad**, 7.1 Panorámica de llevar a cabo los requisitos de información de análisis de seguridad, 7.2 Definir los requisitos de seguridad de la información para el proceso de SGSI, 7.3 Identificar los activos dentro del ámbito SGSI, 7.4 Realizar una evaluación de seguridad de información; **8 Realización de la evaluación de riesgos y planificación de tratamiento de los riesgos,** 8.1 Panorámica de llevar a cabo una evaluación del riesgo y la planificación del tratamiento del riesgo, 8.2 Realizar la evaluación de riesgos, 8.3 Seleccionar los objetivos de control y controles, 8.4 Obtener autorización de la administración para la aplicación y operación de un SGSI; **9 Diseño del SGSI**, 9.1 Descripción del diseño de un SGSI, 9.2 Diseño de seguridad de la información

Otras normas de esta serie: ISO/IEC 27004: Métricas para la gestión de Seguridad de la Información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. **ISO/IEC 27005**: Gestión de riesgos de la Seguridad de la Información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. **ISO/IEC 27006**: Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la Seguridad de la Información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación. **ISO/IEC 27007**: Consistirá en una guía de auditoria de un SGSI. **ISO/IEC 27011**: Consistirá en una guía de gestión de seguridad especifica para telecomunicaciones elaborada conjuntamente con la Unión Internacional de Telecomunicaciones (ITU). **ISO/IEC 27031**: Consistirá en una guía de continuidad del negocio en cuanto a tecnología de la información y comunicaciones. **ISO/IEC 27032**: Consistirá en una guía relativa a la ciber seguridad. **ISO/IEC 27033**: Consistirá en siete partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad de seguridad en redes. Provendrá de la revisión, ampliación y renumeración de la ISO/IEC 18026. **ISO/IEC 27034**: Consistirá en una guía de seguridad en aplicaciones. **ISO/IEC 27799**: Estándar de gestión de seguridad de la información en el sector sanitario y gestión de la salud.

4 Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)

Como antecedentes encontramos que por Decreto 271/94 se establece que es competencia del Poder Ejecutivo fijar una política nacional en materia informática, estableciendo que la Comisión Nacional de informática (CONADI) es el órgano asesor del Poder Ejecutivo en materia informática, la que funcionaba en la orbita de la Oficina de Planeamiento y Presupuesto (OPP) dependiente de la Presidencia de la Republica.

En 1995 se crea el Comité Ejecutivo para la Reforma del Estado (CEPRE) con el cometido central de la reforma y modernización del Estado, abordando aspectos vinculados a los sistemas de información de la Administración Publica.

Por decreto 225/2000 se crea el Comité Nacional para la Sociedad de la información (CNSI) el que tendrá la dirección ejecutiva de los planes para el desarrollo de la sociedad de la información en Uruguay. Sus cometidos, (atribuidos posteriormente a la AGESIC) son: crear las condiciones para definir una política nacional concertada que permita el desarrollo de la sociedad de la información; establecer los lineamientos generales para la definición de una Estrategia Nacional que tenga en cuenta la alfabetización temática, el desarrollo de servicios telemático, la modernización de la Administración Publica, promover el mercados de las telecomunicaciones e Internet y el desarrollo de condiciones de competitividad para el sector Software; etc.

organizacional, 9.3 Diseño de las TIC y seguridad de la información física, 9.4 Diseño SGSI seguridad de la información específica, 9.5 Producir el proyecto final del plan de SGSI.- **Anexos:** Anexo A, Una lista de verificación aplicación SGSI; Anexo B, Funciones y responsabilidades de seguridad de la información; Anexo C, La información sobre la auditoría interna; Anexo D seguridad de la información política de estructuras; Anexo E, Seguimiento y medición del SGSI.

Dependiente del Comité Nacional para la Sociedad de la información se creo una Unidad de Gestión – llamada Uruguay en Red - y un Consorcio Asesor de Empresas, el que aportaría el punto de vista del sector privado.

En marzo del 2005, el Presidente de la Republica crea un Grupo Honorario Asesor de la Presidencia en Tecnologías de la Información (GATI), con el propósito de formular una estrategia para la elaboración de una "Agenda Digital" que permitiera pautar el desarrollo tecnológico del país.

Este grupo recomendó la creación de la Agencia, la que finalmente fue creada por Ley 17.930 Artículo 72 inicialmente como "Agencia para el Desarrollo del Gobierno Electrónico", - denominación fue modificada por Ley 18.046 - a "Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información" y por último - por Ley 18.172 - a *"Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento" (AGESIC)*.

AGESIC, organismo desconcentrado (Art. 54 Ley 18.046 modificativo del Art. 72 Ley 17.930) dentro del Inciso 02 "Presidencia de la República", el programa 007 "Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información" y la unidad ejecutora 010 "Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información", que actuará con autonomía técnica, sin perjuicio de los controles que sean necesarios realizar en los aspectos técnicos por parte de la Unidad Reguladora de Servicios de Comunicaciones. Se comunicará con el Poder Ejecutivo a través de la Oficina de Planeamiento y Presupuesto.

De acuerdo a lo establecido en el Art. 55 de la Ley 18.046 tiene como objetivo la mejora de los servicios al ciudadano utilizando las posibilidades que brindan las tecnologías de la información y de las comunicaciones. Los cometidos asignados por el Poder Ejecutivo a otros órganos u organismos relacionados con áreas de competencia de esta Agencia, se considerarán asignados a ésta.

Asimismo el Art. 118 de la Ley 18.172 agrega un inciso al Art. 55 citado con lo siguiente: "*AGESIC tiene como misión impulsar el avance de la sociedad de la información y del conocimiento, promoviendo que las personas, las empresas y el Gobierno realicen el mejor uso de las tecnologías de la información y las comunicaciones. Asimismo, planificará y coordinará proyectos en el área de Gobierno Electrónico, como base para la transformación y una mayor transparencia del Estado. A los efectos de promover el establecimiento de seguridades que hagan confiable el uso de las tecnologías de la información*, ***la Agencia tiene entre sus cometidos concebir y desarrollar una política nacional en temas de seguridad de la información, que permitan la prevención, detección y respuesta frente a incidentes que puedan afectar los activos críticos del país"***.

Por Decreto 205 del 26 de junio del 2006 se establece que la AGESIC tiene como objetivo procurar la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las tecnologías de la información y las comunicaciones (TIC), asimismo impulsara el desarrollo de la Sociedad de la información en el Uruguay con énfasis en la inclusión práctica digital de sus habitantes y el fortalecimientos de las habilidades de la sociedad en la utilización de las tecnologías.

Dentro de sus cometidos, dicho decreto establece: crear las condiciones para definir una política nacional concertada que permita el desarrollo del Gobierno Electrónico, controlar la ejecución del plan, dirigir actividades de difusión, evaluar avances y resultados, coordinar la instrumentación de las estrategias tecnológicas definidas y establecer pautas necesarias para su aplicación, apoyar y fomentar las acciones basadas en dichas tecnologías que tiendan a mejorar los servicios y la eficiencia operativa de los diferentes organismos del Estado, proponer, coordinar y desarrollar los proyectos basados en tecnología de la información que abarquen horizontalmente a las diferentes reparticiones, desarrollar planes y coordinar acciones para mejorar la inclusión digital de los ciudadanos, coordinación internacional.

En el Art. 119 de la Ley 18.172 Se crea el Consejo Asesor Honorario de Seguridad Informática, que apoyara a la AGESIC en la materia.

Por Ley 18.362 se crean dos organismos:

1. en el Art. 72 se crean en la AGESIC, la ***Dirección de Derechos Ciudadanos*** que tendrá por cometidos la atención de consultas, asesoramiento en materia de protección de datos personales y de acceso a la información pública ,
2. en el Art. 73 el ***"Centro Nacional de Respuesta a Incidentes de Seguridad Informática" (CERTuy),*** con el objetivo de regular la protección de los activos de información críticos del Estado, de acuerdo a los criterios que sugiera el Consejo Honorario de Seguridad Informática en agosto de 2007. Tendrá como cometido difundir las mejores prácticas en el tema, centralizar, coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan.

Asimismo en el Art. 74 de la Ley 18.362 se faculta a la AGESIC a apercibir directamente a los organismos que no cumplan con las normas y estándares en tecnologías de la información establecidas por la normativa vigente, en lo que ***refiera a seguridad de los activos de la información, políticas de acceso, interoperabilidad e integración de datos***.

De lo dispuesto en la Agenda Digital Uruguay 2008 - 2010 para la Sociedad de la Información y el Conocimiento, surge que la misma se encuentra estructurada en torno a la agrupación de los objetivos, entre otros, de Gobierno Electrónico e Institucionalización y Marco Normativo, y se desprende que dentro del primero uno de sus objetivos es "Promover las mejores practicas dentro de las Instituciones Publicas" y dentro del segundo se establece como objetivo: 1. Tener aprobados y reglamentados al 2010 los siguientes proyectos de Ley: Ley de Privacidad / Protección de Datos Personales, Ley de Acceso a la información Publica, Ley de Autenticación de Personas y Documentos, Ley de Regulación de Firma Electrónica, Ley General de Comercio y Compras Electrónicas y 2. "Tener operativa las siguientes unidades: Unidad de protección de Datos Personales, Unidad de Acceso a la información Publica y el Centro de Respuesta a Incidentes Informáticos (CERTuy)"

La AGESIC aprobó el Plan Estratégico el que incluye como líneas estratégicas dentro del capitulo de Eficiencia en la Gestión Publica: establecer políticas, normas y estándares informáticos en el Estado y fiscalizar su cumplimiento. Como Objetivo, del Gobierno Electrónico, establece que le corresponde coordinar y participar en la coordinación de Proyectos específicos asociados al Gobierno Electrónico, entre otros en seguridad informática. Asimismo dentro del ítem Marco Institucional – establecer procedimientos de regulación – encontramos el ítem Seguridad Informática CSIRT Nacional.

Con posterioridad la AGESIC establece la política de Seguridad de la información para los Organismos de la Administración Publica. Dentro de dicho documento se reconoce la importancia de identificar y proteger los activos de información de cada Organismo. Se evitará la destrucción, divulgación, modificación y utilización no autorizada de toda información, comprometiéndose a desarrollar, implantar, mantener y mejorar **continuamente un Sistema de Gestión de Seguridad de la información (SGSI).**

Un SGSI es un conjunto de políticas y procedimientos cuyo objetivo es "administrar la Seguridad de la Información de la Organización". El mismo proporciona una metodología sistemática, documentada, fuertemente enfocada en los riesgos que pueda enfrentar la Organización Mediante un estudio de riesgos, la Organización identifica las brechas de seguridad que posee. Poniendo foco en ello, se eligen las medidas de seguridad y se llevan adelante.

El propósito de un Sistema de Gestión de la Seguridad de la Información, es garantizar que los riesgos sean conocidos y gestionados por la organización de forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en el entorno

y las tecnologías. De esta manera se logra la confiabilidad, integridad y disponibilidad de los activos de la Organización.

5 Principios y líneas estratégicas para el Gobierno en Red.

En el Plan Estratégico, aprobado por el decreto 450/2009, se establece que el Gobierno Electrónico "avanza en el uso de las tecnologías con la finalidad de construir una Administración Publica enfocada al ciudadano, siempre accesible y mas cercana". Se lo define como **el uso de las tecnologías y de la comunicación (TIC) en los órganos de la Administración Pública para mejorar la información y los servicios ofrecidos a los ciudadanos, oriental la eficacia y eficiencia de la gestión publica e incrementar sustantivamente la transparencia del sector público y la participación del ciudadano**.

El Gobierno en red agrega que el **Estado interactúe frente al ciudadano como una unidad**, optimizando procedimientos, e integrando los procesos administrativos entre los distintos organismos. En concepto de Gobierno en Red implica y obliga a la integración tecnológica. Tal integración se lograra al establecer un marco de referencia en base a principios y líneas estratégicas de donde surjan los criterios de aplicación de esas tecnologías, priorización de planes, como para medir resultados de los mismos.

Los principios establecidos son: Principio de Igualdad, Principio de Transparencia, Principio de Accesibilidad, Principio de Eficiencia y Eficacia, Principio de cooperación e integralidad, Principio de Confianza y Seguridad y Principio de Neutralidad tecnológica.

*Respecto al Principio de Seguridad establece: la Administración Pública deberá garantizar un nivel adecuado de integridad, disponibilidad y confiabilidad en la gestión de la información y los servicios que se realicen a través de medios electrónico***s**.

Las líneas estratégicas son: Foco en el Ciudadano, Acceso Universal (accesibilidad, usabilidad, disponibilidad multicanal), Especialización y alineamiento Estratégico, Sustentabilidad y generación de capacidades, Seguridad, Interoperabilidad (organizacional, semántica y técnica), Optimización de recursos TIC, Apoyo a la Industria Nacional e Innovación.

Con respecto a la línea Estratégica Seguridad, establece: Se deberá proveer una efectiva gestión de seguridad para proteger los activos de información y minimizar el impacto en los servicios causados por vulnerabilidades o incidentes de seguridad.

6 CERTuy.-

De acuerdo a lo establecido por el decreto 451/09 reglamentario del Art. 73 de la Ley 13.362, como ámbito objetivo a cargo de la AGESIC a través del CERTuy el proteger los sistemas informáticos que soporten activos de información críticos del Estado, así como los sistemas circundantes a estas; y como ámbito subjetivo, será de aplicación al Estado.

El Art. 3 contiene un conjunto de definiciones entre las cuales encontramos:

1) literal c) **Evento de Seguridad Informática**: es una ocurrencia identificada de un estado de un sistema, servicio a red que indica una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad y
2) literal d) **Incidente de Seguridad Informática** es una violación o amenaza inminente de violación a una política de seguridad de la información implícita o explicita, así como un hecho que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad).

El CERTtuy (Art. 4) tiene como cometidos: Asistir en la respuesta a incidentes de seguridad informática a los organismos estatales afectados, coordinar con los responsables de seguridad de la información de los organismos para prevención, detección, manejo y recopilación de información sobre incidentes de seguridad, colaborar y proponer normas que contribuyan a aumentar los niveles de seguridad, asesorar, difundir, desarrollar herramientas, técnicas de protección, alertar de amenazas y vulnerabilidades, coordinar planes de recuperación de desastres, realizar análisis forenses de los incidentes, centralizar reportes, llevar registros de los incidentes ocurridos, fomentar desarrollo de capacidades y buenas practicas, interactuar como interlocutor con otros organismos naciones o internacionales de igual naturaleza.

Se establece que a los efectos de cumplir sus cometidos podrá (Art. 5) elaborar y difundir recomendaciones, buenas practicas, estándares, alertar sobre incidentes, mantener comunicación con los organismos durante los mismos, capacitar funcionarios, hacer actividades de difusión, emitir opinión cuando le sea solicitada.

Asimismo se establecen obligaciones y procedimientos para el ejercicio de las tareas preventivas (Art. 7 y ss.) tanto para el CERTuy como para las Organizaciones Estatales. **Del primero**: intervenir ante un posible incidente, guardar reserva, llevar registros de reportes, clasificarlos los incidentes según su tipo y severidad, realizar un diagnostico, procurara recuperar los servicios afectados, identificar y mitigar la causa del indicente, preservar la información forense y proveer políticas preventivas, elaborar un informe de lo actuado, publicar recomendaciones, solicitar al Consejo Honorario de la AGESIC, que se dispongan inspecciones, elaborar los informes de las mismas; y **de los segundos**: informar de forma completa e inmediata la existencia de un potencial incidente de seguridad, adoptar medidas de seguridad suficientes para proteger sus activos de información críticos, responder por la integridad de la información generada o en su poder, reparar los daños, consentir la inspección.

7 Políticas de Seguridad de la Información para los Organismos de la Administración Pública

El Art. 1 del decreto 452/009 establece que las Unidades Ejecutoras de los Incisos 02 a 15 del Presupuesto Nacional, **deberán adoptar en forma obligatoria una Política de Seguridad de la Información**, tomando como base la que se incorpora por este decreto en su anexo, con propósito de impulsar un Sistema de Gestión de Seguridad de la Información (SGSI).

Asimismo se exhorta a los Gobiernos Departamentales, los Entes Autónomos, los Servicios Descentralizados y en general a todos los Órganos del Estado adoptar las mismas.

La Política instaurada dispone, que la Dirección del Organismo reconoce la importancia de identificar y proteger los activos de información, que evitara su destrucción, divulgación, modificación y utilización no autorizada, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

Brinda los caracteres básicos de la Seguridad: 1. la preservación de su confidencialidad, 2. su integridad y 3. su disponibilidad.

Establece que la Seguridad se consigue implantando un conjunto adecuado de controles, que deben estar claramente establecidos y difundidos, como políticas, procedimientos, estructuras organizativas, software, e infraestructura.

Cada Organismo designara un Responsable de la Seguridad de la Información, a cuyo cargo se encontrara la implementación y mantenimiento del SGSI.

Tiene especial relieve la necesidad de que la Política de Seguridad debe ser conocida y cumplida por todo el personal del Organismo independientemente del cargo que desempeñe y de su situación contractual. Incluirá instrumentación de sanciones.

El Organismo deberá establecer objetivos anuales con relación a la Seguridad de la Información, desarrollar un proceso de evaluación y tratamiento de riesgos, implementar acciones correctivas y preventivas, elaborar y actualizar un plan de acción; clasificar y proteger la información de acuerdo a la normativa vigente y a los criterios de valoración que para el Organismo posee; cumplir con los requisitos del servicio, legales o reglamentarias y las obligaciones contractuales de seguridad; concientizar y capacitar al personal; contar con una política de gestión de incidentes de seguridad de acuerdo a los lineamiento del CERTuy; establecer la obligación para cada funcionario de reportar incidentes, establecer los medios necesarios para garantizar la continuidad de las operaciones del Organismo.

8 Conclusión

Si bien en Uruguay existieron diversas normas jurídicas, las que marcan el inicio de un proceso desde finales de los años 80, es dentro de lo últimos cinco años que contamos con normativa de rango legal y reglamentario que trata la "Seguridad de la Información" en forma sistemática y estructurada, que han desarrollado y perfeccionado el marco jurídico respecto al tema.

9 Anexo Normativo Cronológico

1) **Ley 15.298** del 7 de julio de 1982: Sistema Nacional de Medidas.
2) **Ley 15.982 (Código General del Proceso)** de 14 de noviembre de 1988, en cuanto al régimen de admisibilidad ("podrán utilizarse otros medios probatorios no prohibidos por la regla de Derecho, Art. 146.2) y de valoración de la prueba (Art. 170 y 140).
3) **Art. 129 Ley 16.002** del 25 de noviembre de 1988: valor probatorio (prueba tasada) de documentación transmitida a distancia.- **Art. 130**: penalización para quien transmitiera un documento infiel[13].-
4) **Decreto 500/91** 27 de setiembre de 1991, modernización del Procedimiento Administrativo. (Modificado por decreto 420/2007 del 7 de noviembre del 2007)
5) **Decreto 271/1994** del 9 de junio de 1994: Creación de la Comisión Nacional de Informática (CONADI)
6) **Art. 84 Ley 16.713** del 3 de septiembre de 1995: sustitución de firma autógrafa por signos o contraseñas mecánica o electrónicamente en cheques del Banco de Previsión Social.
7) **Art. 694 a 697** [14] **Ley 16.736** del 5 de enero de 1996 aplicación de medios informáticos por las Administraciones Públicas.
8) **Art. 703 Ley 16.736** del 5 de enero del 1996: Creación del Comité Ejecutivo para la Reforma del Estado (CEPRE)
9) **Decreto 285/97** del 13 de agosto de 1997

[13] derogado por Ley 18.600 Art. 28

[14] Art. 697 derogado por Ley 18.600 Art. 28

10) **Decreto 65/98** del 10 de marzo de 1998 reglamentación de medios electrónicos de transmisión, almacenamiento y manejo de documentos en la Administración Publica (Ley 16.736)[15]

11) **Decreto 312/98** del 3 de noviembre de 1998 regula firma electrónica en el Documento Único Aduanero.

12) **Resolución del Poder Ejecutivo 1177/99** del 15 de diciembre de 1999: aprobación de un sistema de pago por transferencia electrónica a proveedores del Estado.

13) **Art. 25 Ley 17.243** del 29 de junio del 2000: Sistema Informático del Estado, autorización del uso de firma electrónica, equivalencia a firma autógrafa, implantación del expediente electrónico.[16]

14) **Ley 17.250** del 11 de agosto del 2000, Consumidor electrónico: Derecho de retracto

15) **Art. 65 de Ley 17.292** del 25 de enero del 2001, Ley de Administración Publica y empleo, fomento y mejoras, capitulo Zona Franca (sustituye Art. 2 Ley 15921) emisión de certificados digitales

16) **Decreto 225/00** del 8 de agosto del 2000: Creación del Comité Nacional para la Sociedad de la Información (CNSI)

17) **Decreto 83/01** del 8 de marzo del 2001: En cumplimiento del Art. 15 del Dec. 65/98, se dictan normas relativas a la determinación periódica de los métodos técnicos de almacenamiento, reproducción y transmisión telemática de documentos. [17]

18) **Decreto 66/02** del 26 de febrero del 2002: obligación de publicar en sitios Web los pliegos de bases y condiciones particulares de las licitaciones públicas y abreviadas de los Organismos Públicos. (decretos 526/03 del 18 de diciembre del 2003, y 175/04 del 26 de mayo del 2004)

19) **Decreto 289/02** del 30 de julio del 2002 dispuso el diseño, desarrollo e implementación del Sistema de Compras y Contrataciones Estatales (SICE)

20) **Art. 3 y 29 de la Ley 17.616** del 10 de enero del 2003: Derechos de autor y conexos, referencia a software.

---

[15] En su Art. 15 El Poder Ejecutivo … determinara periódicamente, en consideración a la evolución de la tecnología disponible, los medios técnicos de almacenamiento, reproducción, y transmisión telemática de documentos, que, por su naturaleza o por la eficacia de los procedimientos de control aplicables **ofrezca n protección adecuada contra la perdida o adulteración de la información almacenada, reproducida y/o transmitida**. Art. 20 A efectos de dotar de **seguridad y certeza la gestión del sistema que se reglamenta**, será responsabilidad de cada organismo que dirija un proyecto que utilice la tecnología de claves publica y clave privada, determinar y documentar la forma de administración de la misma.

[16] derogado por Ley 18.600 Art. 28

[17] Se establece que los medios de almacenamiento que el Poder Ejecutivo determine deben **asegurar una adecuada protección contra la perdida o adulteración de la información** almacenada, reproducida y/o transmitida. Que se entiende oportuna la inclusión de recomendaciones que permitan a los Centros de Cómputos de los distintos organismos del Estado, **implementar medidas de seguridad y resguardo de la información**. Que la calidad de los medios físicos a emplearse como soporte, así como de las técnicas de control de calidad en los procesos de grabado y del monitoreo periódico de la calidad de lectura de las copias, con el **objetivo de recuperación de la información**. Que es oportuno el almacenamiento no solo de los datos sino también del software empleado de forma de acceder a los mismos desde sus propios archivos.

21) **Decreto 382/03** del 17 de setiembre del 2003. Reglamentación del uso de la Firma Digital (reglamentación de Art. 129 Ley 16.002, los Art.. 694 a 697 Ley 16.736 y el Art.. 25 Ley 17.243, en cuanto prevén el uso de medios informáticos y telemáticos)[18]

22) **Decreto 154/04 del 3 de mayo del 2004** Reglamentación Ley 17.616

23) **Resolución del Poder Ejecutivo del 18 de marzo del 2005**: Creación del Grupo Honorario Asesor de la Presidencia de la Republica en tecnologías de la Información (GATI)

24) **Art. 70 Ley 17.930** del 19 de diciembre del 2005, Comete a la Oficina de Planeamiento y Presupuesto y a la Oficina de Servicio Civil el programa de transformación del Estado y verificar el cumplimiento de las metas fijadas al respecto. Asimismo el Art. 71 traslada las atribuciones del CEPRE los programas "Planificación del Desarrollo y Asesoramiento para el Sector Publico" y "Administración y Control del Servicio Civil".

25) **Art. 72 Ley 17.930** del 19 de diciembre del 2005: Creación de Agencia para el Desarrollo del Gobierno Electrónico.

26) **Art. 175 a 179 Ley 17.930** del 19 de diciembre del 2005 creación del Instituto Nacional de Calidad.

27) **Art. 256 Ley 17.930:** Agencia Nacional de Innovación

28) **Decreto 205/06** del 26 de junio del 2006

29) **Art. 55 de la Ley 18.046** del 24 de octubre del 2006

30) Plan Estratégico de la AGESIC

31) **Ley 18.084** del 28 de diciembre de 2006. Establece los cometidos de la Agencia Nacional de Investigación e Innovación ANII

32) **Art. 118 de la Ley 18.172** del 31 de agosto del 2007

33) **Art. 329 y 330 Ley 18.72** del 31 de agosto del 2007.- Creación del Registro de Prestadores de Servicios de Certificación que estará a cargo de la Unidad Reguladora de Servicios de Comunicaciones (URSEC), y facultades. [19]

34) Agenda Digital Uruguay 2008-2009

35) **Decreto 17/08** del 16 de enero de 2008 cometidos del Instituto Nacional de Calidad (INACAL)

36) **Decretos 301/08** del 23 de junio del 2008, estructura de puestos de trabajo de AGESIC, modificados por **Decreto 371/08** del 4 de agosto del 2008 y por **Decreto 618/08** del 12 de diciembre del 2008

37) **Ley 18.220** del 20 de diciembre de 2007: Sistema Nacional de Archivos

38) **Ley 18.237** del 26 de diciembre del 2007: Expediente electrónico en el Poder Judicial. Notificaciones Electrónicas.

39) **Ley 18.331** del 11 de agosto de 2008 Protección de Datos Personales y Acción de Habeas Data. (deroga Ley 17.838 del 24/9/2004)

---

[18] Establece que con la sanción del artículo 25 de la Ley 17.243 se reconoce el empleo de la firma digital y su eficacia jurídica para otorgar **seguridad a las transacciones electrónicas**, promoviendo el comercio electrónico seguro, de modo de permitir la identificación en forma confiable de las personas que realicen transacciones electrónicas. Que asimismo, la sanción del artículo 129 de la ley 16.002 y de los artículos 694 a 697 de la ley N° 16.736 impulsa la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información y posibilitar la **realización de trámites por Internet de forma segura.**

[19] Derogados Ley 18.600 Art. 28

40) **Decreto 664/08** del 22 de diciembre del 2008. Reglamenta Ley 18.331. Creación del Registro de Base de Datos Personales a cargo de la Unidad Reguladores y de control de Datos Personales.-

41) **Art. 72 y 73 Ley 18.362** del 6 de octubre del 2008

42) **Ley 18.381** del 17 de octubre del 2008, Derecho de Acceso a la Información Publica

43) **Ley 18.383** del 7 de octubre del 2008 sustituye el Art. 217 del Código Penal, delito de atentado a regularidad de las comunicaciones

44) **Decreto 414/09** del 31 de agosto del 2009 y **Decreto 437/09** del 28 de setiembre del 2009. Reglamentan Ley 18.331

45) **Decreto 484/09** del 3 de noviembre del 2009: Reglamenta Ley 18.381

46) **Ley 18.600** del 21 de setiembre del 2009 Reconócese la admisibilidad, la validez y la eficacia jurídicas del documento electrónico y de la firma electrónica. Derogaciones: Art. 129 y 130 Ley 16002, 697 Ley 16736, 25 Ley 17243, 329 y 330 Ley 18172 y demás normas que se opongan.

47) **Decreto 450/09** del 28 de setiembre de 2009 aprueba el documento Principios y Líneas Estratégicas para el Gobierno en Red

48) **Decreto 451/09** del 28 de setiembre de 2009, Se reglamenta el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)

49) **Decreto 452/09** del 28 de setiembre de 2009, Adopción de una Política de Seguridad de la Información para Organismos de la Administración Publica

50) **Decreto 82/10** del 25 de febrero del 2010, aprobación del Plan Estratégico Nacional de Ciencia, Tecnología e Innovación (PENCTI)

51) **Decreto 89/10** del 26 de febrero del 2010, Creación del Sistema Uruguayo de Normalización, Acreditación, Metrologia y Evaluación de la Conformidad (SUNAMEC)

10 Fuentes - Conferencias - Bibliografía

1) Sociedad del Conocimiento y Derecho, Prof. Fernando Galindo, Contratación Electrónica, AEU, 2006
2) Desafíos Jurídicos relacionados al Gobierno Electrónico, con especial referencia a la Administración electrónica, Dr. Carlos E. Delpiazzo, Síntesis de la exposición pronunciada en el Seminario "Políticas Publicas para el Gobierno Electrónico", 23 de marzo del 2006.
3) Informática y Gobierno, Alternativas al desarrollo del Gobierno Electrónico en el Uruguay. Dra. Laura Nahabetian Brunet. Derecho Informático FCU Tomo V
4) El E – Procurement o el nuevo rostro de la contratación Administrativa. Dr. Carlos E Delpiazzo. Derecho Informático FCU Tomo III
5) Experiencias de E – Government en Europa. Dra. Esc. María José Viega. Derecho Administrativo FCU Tomo III
6) El principio de Seguridad Jurídica en el Mundo Virtual, Dr. Carlos Delpiazzo. Derecho Informático FCU Tomo VII
7) Firma Electrónica, Esc. Aída Noblia, Contratación Electrónica AEU, 2006
8) Nuevas Tecnologías de la información y Comunicación (NTIC´s) y Derecho, Esc. Aída Noblia. 2009
9) Seguridad en las Transacciones Administrativas Dra. Maricament Pascale. Derecho Informático FCU Tomo IV

10) El Sistema de Gestión de Seguridad de a información. La nueva norma UNE 71502. Códigos de buenas practicas de seguridad UNE ISO/IEC 17799, Antonio Villalon Huerta Grupo S2, 30 de setiembre del 2004, Valencia.
11) Seguridad informática y la Norma ISO 17799, Ing. Leonardo Berro. Derecho Informático FCU Tomo V
12) Aspectos de la Seguridad en la Gestión Administrativa, Dr. Héctor Delpiano. Derecho Informático Tomo IV
13) Gobierno Progresista: Los primeros pasos hacia la sociedad de la información. información. Roberto Elissalde (diciembre 2005)
14) El gobierno electrónico en la Agenda de la Transformación del Estado. Ing. Virginia Pardo, A/P Federico Monteverde, y A/S A/M Mauro D Ríos. (Conferencia obtenida en Internet)
15) Conferencia Seguridad de la información Setiembre 2009 José Clastornik, AGESIC
16) Conferencia Buenas Practicas en Seguridad de la información, Expositores, AGESIC
17) Conferencia Sistema de Gestión de Seguridad de la información, AGESIC
18) Conferencia Sistema de Gestión de Seguridad de la información, Aspecto Normativo. UNIT ISO/IEC 27000, AGESIC
19) Firma Electrónica Digital Ley 18.600, Esc. Aída Noblia y Marcelo Rivero, Taller de la Comisión de Derecho Informática, AEU marzo 2010
20) Paginas Web: www.agesic.gub.uy, www.cert.uy, www.datospersonales.gub.uy, www.informacionpublica.gub.uy

11 Indice de contenidos