



Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

Buenas Prácticas en Seguridad de la Información

**Expositor:
A/S Glenda Garcés**

ÍNDICE

- Introducción
- Marco de Referencia Normativo
- Política de Seguridad de la Información
- Directriz para la implementación de la Ley 18.331

BUENAS PRÁCTICAS en SEGURIDAD de la INFORMACIÓN

Existe una realidad dispar en materia de seguridad de la información en el Estado Uruguayo.

Contamos con organizaciones que tienen actualmente SGSI implantados, conforme a normas internacionalmente aceptadas.

Así como organismos que aún no han identificado la importancia de estos temas.

OBJETIVO

- Mejorar la seguridad de la información en las dependencias Estatales.
- Facilitar herramientas que ayuden en la implantación de buenas prácticas de seguridad de la información.
- Preservar la confidencialidad, integridad y disponibilidad de los Activos de información del Estado.

PRODUCTOS

- Catálogo de Normas de Seguridad de la Información
- Modelo de Política de Seguridad de la Información
- Directrices para la aplicación de la Ley 18.331 según la familia de Normas ISO/IEC 27000

CATÁLOGO de NORMAS de SEGURIDAD de la INFORMACIÓN

El Catálogo de Normas en Seguridad de la Información, contendrá un conjunto mínimo de especificaciones, normas y publicaciones en materia de Seguridad de la Información.

Los Organismos de la administración pública deberán tomar como referencia las normas detalladas en este documento, a fin de gestionar la seguridad de la información en cada Organismo.

La serie ISO/IEC 27000 contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

Norma	Propósito
ISO/IEC 27000:2009	Ofrece una visión general de los sistemas de gestión de seguridad de la información y define los términos relacionados. Se encuentra en proceso de homologación nacional como UNIT-ISOMEC 27000 (disponible a partir de agosto de 2009).
ISO/IEC 27001:2005	Norma que especifica los requisitos para la implantación de un SGSI, es una norma certificable. Homologada a nivel nacional como UNIT-ISOMEC 27001:2005.
ISO/IEC 27002:2005	Código de buenas prácticas para la gestión de seguridad de la información. Homologada a nivel nacional como UNIT-ISOMEC 27001:2005.
ISO/IEC 27003	Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Se encuentra en fase de desarrollo.
ISO/IEC 27004	Métricas para la gestión de seguridad de la información, proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Se encuentra en fase de desarrollo.
ISO/IEC 27005:2008	Gestión de riesgos en seguridad de la información, proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, como soporte al proceso de gestión de riesgos de la norma ISO/IEC 27001. Homologada a nivel nacional como UNIT-ISOMEC 27005:2008.
ISO/IEC 27006:2007	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información.
ISO/IEC 27007	Directrices para auditar Sistemas de Gestión de Seguridad de la Información. Se encuentra en elaboración.

Ag

Norma	Propósito
ISO/IEC 27031	En fase de desarrollo. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
ISO/IEC 27032	En fase de desarrollo. Consistirá en una guía relativa a la ciberseguridad.
ISO/IEC 27033	En fase de desarrollo. Es una norma consistente en 7 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 en redes. Provenirá de la revisión, ampliación y renumeración de ISO/IEC 18028.
ISO/IEC 27034	En fase de desarrollo. Consistirá en una guía de seguridad en aplicaciones.
ISO/IEC TR 18044:2004 (ISO/IEC 27035)	Provee asesoramiento y guía en la gestión de incidentes de seguridad de la información. Se encuentra actualmente en revisión y está planificado que la nueva versión se publique bajo la numeración ISO/IEC 27035. Homologada a nivel nacional como UNIT-ISO/IEC TR 18044:2004
ISO 27799:2008	Publicada el 12 de Junio de 2008. Es una norma de gestión de seguridad de la información en el sector salud aplicando ISO/IEC 27002:2005.

DECRETOS APROBADOS

El Presidente de la República en Consejo de Ministros decretó el pasado 28 de setiembre los documentos de:

- **Principios y Líneas Estratégicas** para el Gobierno en Red
- La regularización del **Centro Nacional de Respuesta e Incidencias de Seguridad Informática**
- La adopción de una **Política de Seguridad** de la información para organismos de la Administración Pública.

POLÍTICA de SEGURIDAD de la INFORMACIÓN

Se ha elaborado un modelo de Política de Seguridad de la Información para los Organismos del Estado, con el fin recomendar la implementación un Sistema de Gestión de Seguridad de la Información en la administración pública.

Las Direcciones de los Organismos, serán quienes tengan el cometido de reconocer la importancia, de identificar y proteger los activos de información de cada Organismo a través de la aprobación y ejecución de esta política.

POLÍTICA de SEGURIDAD de la INFORMACIÓN

La Política de Seguridad de la Información, es de aplicación obligatoria y deberá ser conocida y cumplida por todo el personal de los Organismos, integrándose a la normativa básica del Organismo, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento.

ANEXO I

Política de Seguridad de la Información para Organismos de la Administración Pública

La Dirección del Organismo reconoce la importancia de identificar y proteger los activos de información del Organismo. Para ello, 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.

La Dirección del Organismo declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, procedimientos, estructuras organizativas, software e infraestructura. Estos controles deberán ser establecidos para asegurar los objetivos de seguridad del Organismo.

El Organismo designará un Responsable de la Seguridad de la Información, quien se encargará de la guía, implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información.

La presente Política de Seguridad de la Información debe ser conocida y cumplida por todo el personal del Organismo, independiente del cargo que desempeñe y de su situación contractual.

Esta Política de Seguridad de la Información se integrará a la normativa básica del Organismo, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de la presente política, así como de los documentos relacionados a esta.

Es política del Organismo:

- Establecer objetivos anuales con relación a la Seguridad de la Información.
- Desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad, y de acuerdo a su resultado implementar las acciones correctivas y preventivas correspondientes, así como elaborar y actualizar el plan de acción.

- Clasificar y proteger la información de acuerdo a la normativa vigente y a los criterios de valoración en relación a la importancia que posee para el Organismo.
- Cumplir con los requisitos del servicio, legales o reglamentarios y las obligaciones contractuales de seguridad.
- Brindar concientización y formación en materia de seguridad de la información a todo el personal.
- Contar con una política de gestión de incidentes de seguridad de la información de acuerdo a los lineamientos establecidos por el CERTuy.
- Establecer que todo el personal es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.
- Establecer los medios necesarios para garantizar la continuidad de las operaciones del Organismo.

DIRECTRIZ para la aplicación Ley 18.331

Con el objeto de facilitar a los directores de empresas públicas y privadas la adopción de la ley y su correspondiente reglamentación, es que AGESIC elaboró y pondrá a disposición una guía con el propósito de facilitar el desarrollo y cumplimiento de la normativa sobre protección de datos personales.

Con esta directriz se pretende, en base a lo dispuesto por la Ley, acercar buenas prácticas aceptadas internacionalmente en materia de seguridad de la información a nuestras organizaciones y empresas. Es así que se establece una relación directa de los principios desarrollados en la Ley contra los controles de la norma UNIT-ISO/IEC 27002.

PRINCIPIOS DE LA LEY N° 18.331

LEGALIDAD

SEGURIDAD

VERACIDAD

RESPONSABILIDAD

FINALIDAD

RESERVA

**PREVIO
CONSENTIMIENTO
INFORMADO**

PRINCIPIO DE LEGALIDAD

- La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia.
- Referencias a la norma UNIT-ISO/IEC 27002:2005
 - 7.1.1 Inventario de activos
 - 7.2 Clasificación de la información

COMO SEGUIMOS

Los documentos relacionados a este proyecto estarán disponibles en el sitio de AGESIC www.agesic.gub.uy en su versión imprimible desde Diciembre del 2009.

A partir de eso se desarrollarán actividades de difusión y capacitación que permitirán a los organismos y empresas interesadas profundizar en cada uno de los conceptos.

INFORMACIÓN de CONTACTO

Por información sobre este proyecto consultar en:

normasti@agesic.gub.uy

Preguntas?

Esperamos tus comentarios, aportes y sugerencias.

consultas@agesic.gub.uy

Muchas gracias !!

www.agesic.gub.uy