

## Puesta en marcha y operación de un Sistema de Gestión de Seguridad de la Información



1

## Agenda

- Sistema de Información
- Rol de la información en la gestión de la organización
- Seguridad de la información
- Riesgos e impacto
- Evaluación y tratamiento de riesgos
- Marco normativo
- Objetivos de una Gerencia de Seguridad de la Información
- Clasificación de la información<sub>2</sub>

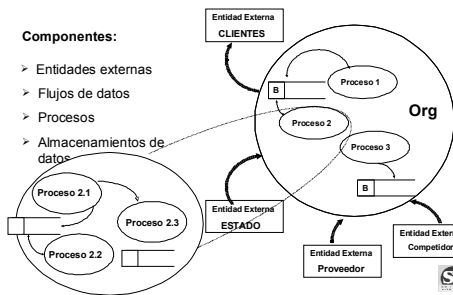


## Sistema de Información

ANTEL

### Componentes:

- Entidades externas
- Flujos de datos
- Procesos
- Almacenamientos de datos

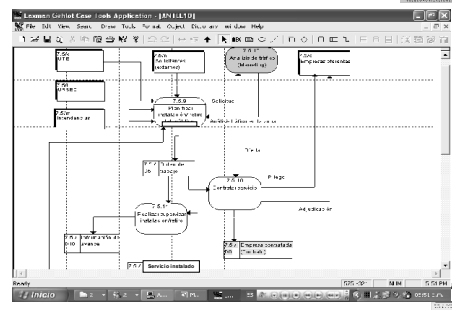


3

Agosto, 2007

## Clasificación de los Procesos

ANTEL



4

Agosto, 2007

## Sistema de Información

ANTEL

### Naturaleza de los recursos (Componentes)

- Recursos Humanos
- Hardware
- Telecomunicaciones
- Software
- Datos

5

Agosto, 2007

## Rol de la información en la gestión

ANTEL

### Operativo

- Facilita la tarea
- Reduce el esfuerzo
- Mejora la calidad
- Hace posible nuestros negocios !!

### Táctico

- Elemento para la supervisión
- Posibilita la mejora continua

### Gerencial



- Apoyo a la toma de decisiones

6


Agosto, 2007



## Ejemplos de Incidentes de Seguridad

- Pérdida de integridad de documentos en el Banco Central de Uruguay
- Pérdida de datos de estudiantes en Instituto Universitario en Uruguay
- Extorsión para evitar difusión de bases de datos de tarjetas de crédito internacionales (American Express y otras...)
- Ataques de Denegación de Servicio a ISP
- Planes comerciales que nos han anticipado¿?
- Phishing, a diversas entidades bancarias en y desde Uruguay.

7   Agosto, 2007

## Seguridad de la Información

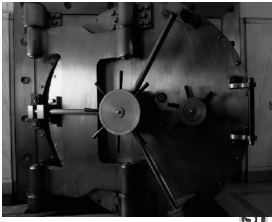




8   Agosto, 2007

## Seguridad de la información

### Definición

- Integridad
- Confidencialidad
- Disponibilidad








9   Agosto, 2007

## Seguridad de la información



### Medidas de seguridad

- Lógicas (*Seguridad lógica*)
- Físicas (*Seguridad física*)
- Ambiental (*Seguridad ambiental*)

10   Agosto, 2007

## Riesgos e impacto

11   Agosto, 2007

## Riesgos e impacto



### Amenazas







#### Inherentes:


- Soporte TI
- RRHH
- Entorno
- Medio ambiente

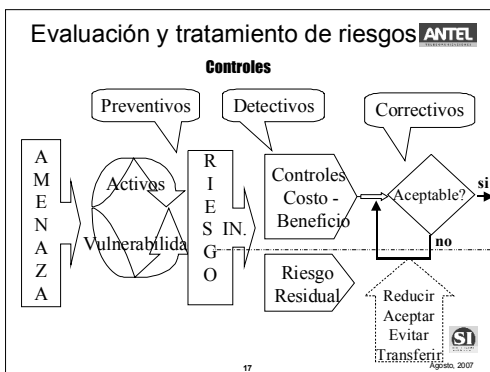
12   Agosto, 2007


Riesgos e impacto		
Amenazas	Origen de la debilidad	Ataque / Falla
 <p>Inherentes:</p> <ul style="list-style-type: none"> <li>• Soporte TI</li> <li>• RRHH</li> <li>• Entorno</li> <li>• Medio ambiente</li> </ul>	 <p>Tecnológico Recursos Humanos Prácticas operativas</p>	<ul style="list-style-type: none"> <li>• Hacking</li> <li>• IP spoofing</li> <li>• Virus</li> <li>• Enmascaramiento</li> <li>• Spamming</li> <li>• Caballo de Troya</li> <li>• Fallas del equipamiento</li> <li>• Falla de las telecomunicaciones</li> <li>• Piratería de software</li> </ul>

Riesgos e impacto		
Amenazas	Origen de la debilidad	Ataque / Falla
 <p>Inherentes:</p> <ul style="list-style-type: none"> <li>• Soporte TI</li> <li>• RRHH</li> <li>• Entorno</li> <li>• Medio ambiente</li> </ul>	 <p>Tecnológico Recursos Humanos Prácticas operativas</p>	<ul style="list-style-type: none"> <li>• Falta de capacitación</li> <li>• Errores</li> <li>• Fraudes</li> <li>• Negligencia</li> </ul>

Riesgos e impacto		
Amenazas	Origen de la debilidad	Ataque / Falla
 <p>Inherentes:</p> <ul style="list-style-type: none"> <li>• Soporte TI</li> <li>• RRHH</li> <li>• Entorno</li> <li>• Medio ambiente</li> </ul>	 <p>Tecnológico Recursos Humanos Prácticas operativas</p>	<ul style="list-style-type: none"> <li>• Caballo de Troya</li> <li>• Ingeniería social</li> <li>• Ataques contra la privacidad de los datos</li> <li>• Fraude operativo</li> <li>• Piratería de software</li> </ul>

Riesgos e Impacto: Costo de la "no seguridad"	
<ul style="list-style-type: none"> <li>➢ Pérdidas, directas o indirectas           <ul style="list-style-type: none"> <li>➢ Pérdidas financieras por indisponibilidades</li> <li>➢ Pérdidas de imagen</li> <li>➢ Pérdida de "resiliencia" organizacional</li> </ul> </li> <li>➢ Implantación de controles           <ul style="list-style-type: none"> <li>➢ Costo asociado al establecimiento de controles del Sistema de Información</li> </ul> </li> <li>➢ Mantenimiento           <ul style="list-style-type: none"> <li>➢ Costo de Mantenimiento de los diferentes repositorios de datos, procedimientos y monitoreos excesivos o duplicados</li> </ul> </li> </ul>	



Evaluación y tratamiento de riesgos	
<ul style="list-style-type: none"> <li>➢ <b>Evaluando el riesgo de seguridad (Norma)</b></li> <li>➢ Se deben identificar, cuantificar, y priorizar los riesgos contra los criterios para la aceptación del riesgo y los objetivos relevantes para la organización</li> <li>➢ Se debe dirigir y determinar la apropiada acción de gestión y las prioridades para gestionar los riesgos de la seguridad de la información y para implementar los controles seleccionados como protección ante estos riesgos</li> <li>➢ Lo que debe incluir :           <ul style="list-style-type: none"> <li>➢ Análisis de riesgos</li> <li>➢ Evaluación de riesgos</li> </ul> </li> </ul>	

## Evaluación y tratamiento de riesgos

### ➤ Se deben implementar controles teniendo en cuenta:

- requisitos y restricciones de la legislación (nacionales e internacionales)
- objetivos de la organización
- requisitos y restricciones operacionales
- costo de la implementación y de la operación
- balancear la inversión en la implementación y la operación de controles contra el daño probable como resultado de fallas de la seguridad



19

Agosto, 2007

## Evaluación y tratamiento de riesgos

### ➤ Tratando los riesgos de seguridad

- Luego se deberá definir que hacer con los riesgos residuales
- Opciones
  - Reducirlo,
  - Aceptarlo,
  - Evitarlo,
  - Transferirlo.



20

Agosto, 2007

## Evaluación y tratamiento de riesgos

➤ Los controles de seguridad de la información deben considerarse en las etapas de especificación de requisitos y de diseño en sistemas y proyectos.

➤ no hacerlo puede dar lugar a costos adicionales y a soluciones menos eficaces, y quizá, en el peor de los casos, inhabilidad de alcanzar la seguridad adecuada.



21

Agosto, 2007

## Evaluación y tratamiento de riesgos

### ➤ Implantación de controles

<b>Impacto</b>	<b>Alto:</b> Información crítica, daño serio, patrimonial
	<b>Medio:</b> Pérdida de información sensible, retraso o interrupción
	<b>Bajo:</b> Pérdida de Información y/o equipamiento no sensitivo
<b>Probabilidad de Ocurrencia</b>	<b>Frecuente:</b> Incidentes repetidos
	<b>Probable:</b> Incidentes aislados
	<b>Ocasional:</b> Sucede alguna vez
	<b>Remoto:</b> Improbable que suceda



22

Agosto, 2007

## Evaluación y tratamiento de riesgos

### ➤ Implantación de controles

**Exposición = Impacto X Probabilidad**

		Impacto		
		Alto	Medio	Bajo
Probabilidad de Ocurrencia	Frecuente			
	Probable			
	Ocasional			
	Remoto			



23

Agosto, 2007

## Marco Normativo: Políticas de Seguridad

➤ Debe realizarse un Documento de Políticas de Seguridad, que permita promover aquellos aspectos que sean relevantes en el análisis de riesgos realizado a los activos.

➤ Entre otros aspectos dichas políticas de Seguridad deben enmarcar las responsabilidades y competencias que debe poseer un "Dueño de la Información", "Administrador de Información" y "Usuario" además de muchos otros roles.

➤ Debe también especificar los comités o grupos que deben desarrollarse y mantenerse, en la estructura organizativa para la correcta implementación de las acciones de seguridad según definan las políticas y las circunstancias.



24

Agosto, 2007

## Marco Normativo



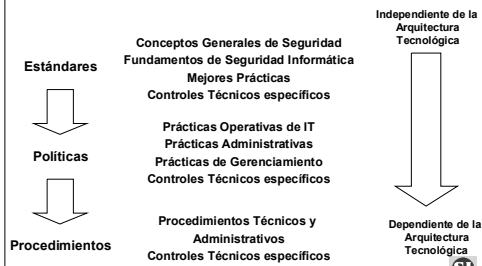
- Políticas de Seguridad de la Información, base para la toma de decisiones en el tema
- Procedimientos de primer nivel, en diferentes fases de implementación en la organización
- Procedimientos de segundo nivel, en general provistos por las Gerencias Operativas
- Manuales de Operación



25

Agosto, 2007

## Marco normativo



26

Agosto, 2007

## Objetivos de una Gerencia de Seguridad de la Información



- Mantener las Políticas de Seguridad y los Procedimientos de Seguridad requeridos para su implantación, en función de los objetivos de negocio de la organización.
- Definir, apoyar en la implementación y velar por el cumplimiento de los controles derivados de los Procedimientos de Seguridad, y de cualquier otro tipo, requeridos para cumplir con el marco normativo antes mencionado.
- Asistir a los empleados atendiendo a consultas de Seguridad que puedan presentarse en cualquier lugar de la organización.
- Promover la concientización continua de todos los involucrados con el Sistema de Información en particular, respecto a los temas de Seguridad de la Información y velar por la implantación de una "cultura de Seguridad".
- Participar en los proyectos que corresponda para garantizar que los mismos incluyan un adecuado control de riesgos, si la implementación de los mismos puede afectar el nivel de seguridad y control de la empresa.
- Proveer un servicio independiente para recabar y administrar adecuadamente los "logs" y otros registros, los cuales servirán como elemento central de controles y eventuales investigaciones



27

Agosto, 2007

## Clasificación de la información



- **Secreta:**
  - Datos que tienen el nivel más limitado de acceso dentro de la organización y requieren un alto grado de integridad. Típicamente son los datos que le causarían mayor daño a la organización en caso de ser revelados a terceras partes no autorizadas.
- **Confidencial:**
  - Datos que pueden tener una utilización menos restrictiva que los anteriores dentro de la organización, pero que de todos modos pueden causar algún nivel de daño en caso de ser revelados a terceras partes no autorizadas.

28

Agosto, 2007

## Clasificación de la información



- **Uso Interno:**
  - Datos que si bien probablemente no causarían un daño importante de ser publicados, igual deben ser mantenidos como privados por otros motivos. Estos datos están típicamente asociados a un área o departamento en particular.
- **Pública:**
  - Los datos públicos son aquellos que tienen el menor nivel de sensibilidad y no deberían causar ningún tipo de impacto para la organización en el caso de ser publicados.



29

Agosto, 2007

The screenshot shows a Microsoft Excel spreadsheet titled "Diccionario" with columns for classification levels (A, E, C, D, E, F, G, H, I, J, K) and rows for various information types. The columns represent different classification levels: A (Uso Interno), E (Confidencial), C (Secreta), D (Confidencial), E (Uso Interno), F (Pública), G (Especial), H (Normal), I (Confidencial), J (Secreta), K (Confidencial).

	A	E	C	D	E	F	G	H	I	J	K
1	Colaboradores	Nombre	Secreta	Confidencial	Uso Interno	Pública	Especial	Normal			
2											
3	D100	Director de cursos									
4	D111	Proceso-DA									
5	D112	Planificación de actividades									
6	D113	Gerencia									
7	D114	Mantenimiento									
8	D115	Gerencia del cliente									
9	D116	Proceso-DA									
10	D117	Uso de recursos									
11	D118	Planificación									
12	D119	Planificación									
13	D120	Cargos por ser visto									
14	D121	Cargos por ser visto									
15	D122	Cargos por ser visto									
16	D123	Cargos por ser visto									
17	D124	Proyectos marplatenses									
18	D125	Proyectos marplatenses									
19	D126	Proyectos marplatenses									
20	D127	Proyectos marplatenses									
21	D128	Proyectos marplatenses									
22	D129	Proyectos marplatenses									
23	D130	Proyectos marplatenses									
24	D131	Proyectos marplatenses									
25	D132	Proyectos marplatenses									
26	D133	Proyectos marplatenses									
27	D134	Proyectos marplatenses									
28	D135	Proyectos marplatenses									
29	D136	Proyectos marplatenses									
30	D137	Proyectos marplatenses									
31	D138	Proyectos marplatenses									
32	D139	Proyectos marplatenses									
33	D140	Proyectos marplatenses									
34	D141	Proyectos marplatenses									
35	D142	Proyectos marplatenses									
36	D143	Proyectos marplatenses									
37	D144	Proyectos marplatenses									
38	D145	Proyectos marplatenses									
39	D146	Proyectos marplatenses									
40	D147	Proyectos marplatenses									
41	D148	Proyectos marplatenses									
42	D149	Proyectos marplatenses									
43	D150	Proyectos marplatenses									
44	D151	Proyectos marplatenses									
45	D152	Proyectos marplatenses									
46	D153	Proyectos marplatenses									
47	D154	Proyectos marplatenses									
48	D155	Proyectos marplatenses									
49	D156	Proyectos marplatenses									
50	D157	Proyectos marplatenses									
51	D158	Proyectos marplatenses									
52	D159	Proyectos marplatenses									
53	D160	Proyectos marplatenses									
54	D161	Proyectos marplatenses									
55	D162	Proyectos marplatenses									
56	D163	Proyectos marplatenses									
57	D164	Proyectos marplatenses									
58	D165	Proyectos marplatenses									
59	D166	Proyectos marplatenses									
60	D167	Proyectos marplatenses									
61	D168	Proyectos marplatenses									
62	D169	Proyectos marplatenses									
63	D170	Proyectos marplatenses									
64	D171	Proyectos marplatenses									
65	D172	Proyectos marplatenses									
66	D173	Proyectos marplatenses									
67	D174	Proyectos marplatenses									
68	D175	Proyectos marplatenses									
69	D176	Proyectos marplatenses									
70	D177	Proyectos marplatenses									
71	D178	Proyectos marplatenses									
72	D179	Proyectos marplatenses									
73	D180	Proyectos marplatenses									
74	D181	Proyectos marplatenses									
75	D182	Proyectos marplatenses									
76	D183	Proyectos marplatenses									
77	D184	Proyectos marplatenses									
78	D185	Proyectos marplatenses									
79	D186	Proyectos marplatenses									
80	D187	Proyectos marplatenses									
81	D188	Proyectos marplatenses									
82	D189	Proyectos marplatenses									
83	D190	Proyectos marplatenses									
84	D191	Proyectos marplatenses									
85	D192	Proyectos marplatenses									
86	D193	Proyectos marplatenses									
87	D194	Proyectos marplatenses									
88	D195	Proyectos marplatenses									
89	D196	Proyectos marplatenses									
90	D197	Proyectos marplatenses									
91	D198	Proyectos marplatenses									
92	D199	Proyectos marplatenses									
93	D200	Proyectos marplatenses									

30

Agosto, 2007

## Tipos de usuarios



- Usuario **Responsable** de la información
- Usuario **Administrador** de la información
- **Usuario** de la información (consulta)



31

Agosto, 2007

## Tipos de usuarios



- Usuario **Responsable** de la información
  - Comprende claramente la naturaleza de la información, pudiendo advertir si la misma está completa y es correcta.
  - En caso de no ser correcta, tiene la capacidad de corregirla en base a su propio conocimiento
  - Es responsable de archivarla, ya sea manualmente o utilizando alguna herramienta de software.
  - Conoce el tiempo de guarda requerido de la información
  - Es el responsable de mantenerla actualizada, y/o supervisar las modificaciones que la misma sufra
  - Es el responsable de autorizar, y eventualmente realizar su eliminación del Sistema de Información en caso que corresponda



32

Agosto, 2007

## Tipos de usuarios



- Usuario **Administrador** de la información
  - Es responsable de instrumentar la custodia de la información, ya sea mediante procedimientos manuales o automáticos.
  - Conoce y/o administra las herramientas mediante las cuales se registra/almacena/procesa/distribuye la información.
  - Posibilita la utilización de las herramientas para realizar altas, bajas y modificaciones sobre la información.
  - Apoya en las tareas de recuperación de la información ante incidentes



33

Agosto, 2007

## Tipos de usuarios



- **Usuario** de la información
  - Son aquellos funcionarios que utilizan en el marco de sus tareas, parte de la información del Sistema de Información de la Organización.



34

Agosto, 2007

## Políticas de Seguridad de la Información: Breves comentarios



- **Propósito y alcance:** La política de Seguridad debe proveer dirección y apoyo a la alta gerencia, establecer un marco de implementación de seguridad y asegurar el cumplimiento de la Seguridad de la Información en la organización.
- **Declaración de la Política:** La política de seguridad de la información, debe proveer una dirección estratégica adecuada para demostrar la importancia de la Seguridad de la Información para los procesos de negocio.



35

Agosto, 2007

## Alcance.



- Establece recomendaciones y principios generales para iniciar, implantar, mantener y mejorar la gestión de la seguridad de la información
- Señala objetivos que proporcionan recomendaciones generales sobre las metas comúnmente aceptadas para la gestión de la seguridad de la información.
- Establece objetivos de control y controles para ser implementados a fin de alcanzar los requisitos identificados por una evaluación del riesgo.
- Es una recomendación práctica para desarrollar normas de seguridad de la organización y una práctica efectiva de la gestión de la misma, así como ayudar a construir confianza en las actividades entre organizaciones



36

Agosto, 2007

## Definiciones.



➤ Definición de términos referenciados en la norma tales como:

- Activo, control, guía,
- eventos, incidentes y políticas de seguridad
- Análisis, evaluación, valoración, gestión y tratamiento de riesgos



37

Agosto, 2007

## Estructura de la Norma.



➤ Contiene 11 cláusulas de control de la seguridad que en su conjunto contienen un total de 39 categorías principales de seguridad y una cláusula introductoria a la evaluación y tratamiento de riesgos.

➤ Cada organización que aplica esta norma debería identificar las cláusulas aplicables, que tan importantes son y su aplicación a los procesos individuales del negocio



38

Agosto, 2007

## Estructura de la Norma



- a) Política de Seguridad
- b) Organización de la Seguridad de la Información
- c) Gestión de Activos
- d) Seguridad de Recursos Humanos
- e) Seguridad Física y del Ambiente
- f) Gestión de Comunicaciones y Operaciones
- g) Control de Acceso
- h) Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información



39

Agosto, 2007

## Estructura de la Norma



- i) Gestión de Incidentes de la Seguridad de la Información
- j) Gestión de la Continuidad del Negocio
- k) Cumplimiento



40

Agosto, 2007

## Muchas gracias



¿Consultas?

Para ubicarnos:

[www.csirt-antel.com.uy](http://www.csirt-antel.com.uy)

[csirt@csirt-antel.com.uy](mailto:csirt@csirt-antel.com.uy)

[eduardo.carozo@csirt-antel.com.uy](mailto:eduardo.carozo@csirt-antel.com.uy)



41

Agosto, 2007