Implantación Exitosa de la Normativa sobre Seguridad de la Información en el Estado Uruguayo

JIAP

Montevideo – Uruguay
17 de Agosto de 2011.

Ing. Reynaldo C. de la Fuente, CISA, CISSP, CRISC, MBA

La situación actual

Veamos otros casos de éxito a nivel Internacional

Otros “Casos de Éxito”

Viewing cable 04MADRID2215, AZNAR KEP

If you are new to th… them with others. S…

Reference ID
04MADRID2215

This record i…
original cabl…

C O N F I D …

SIPDIS

E.O. 12958: …
TAGS: PGOV PR…
SUBJECT: AZNA…
CAMPAIGN CENT…

Classified By…

Dimite por un desliz el jefe antiterrorista británico

Expuso documentos secretos sobre un operativo contra extremistas

LONDRES.– En momentos en que Scotland Yard se encuentra en la mira por varios incidentes que comprometieron su imagen, el jefe de la sección antiterrorista de la institución debió renunciar ayer por haber expuesto ante las cámaras fotográficas un documento secreto sobre un operativo antiterrorista minutos antes de una reunión con el primer ministro, Gordon Brown.

La dimisión ocurrió al día siguiente de que se informara que Scotland Yard sería investigada por la presunta responsabilidad de uno de sus agentes en la muerte de un manifestante durante la última cumbre del G-20 en la capital británica.

La policía decidió anteayer adelantar una redada en el noroeste de Inglaterra en la que detuvo a 12 sospechosos de terrorismo, 11 de los cuales son ciudadanos paquistaníes,

EFE

Quick expone la operación secreta

detención estaba programada para el jueves. Gran Bretaña se encuentra en estado de alerta antiterrorista desde los atentados del 7 de julio de 2005 en Londres, en los que murieron 56 personas, incluidos los cuatro kamikazes.

El primer ministro británico dijo ayer que los presuntos terroristas urdían un “complot terrorista muy grande”, que las fuerzas de seguridad investigaban “desde hacía algún tiempo”. Brown añadió que el gobierno está al tanto de los “vínculos entre terroristas en el Reino Unido y terroristas en Paquistán”, y que hablará con el presidente de ese país, Asif Ali Zardari, para que refuerce la cooperación antiterrorista.

Escándalos y muertes

Este caso pone aún más en aprietos a Scotland Yard, que ya está siendo

Otros “Casos de Éxito”

Inicio

24/06/2011 | ENVIAR | IMPRIMIR

POLICÍA PERUANA PIDE AYUDA AL FBI POR HACKEOS A PÁGINAS WEBS DEL GOBIERNO

Fuentes policiales descartaron que Anonymous, grupo hacker int
o amenazado páginas gubernamentales de varios países, esté detr
comentó que se trata de un grupo nuevo que se autodenomina Pir

Viernes 24 de junio de 2011

La **Policía peruana pidió ayuda al FBI estadounidense para ubicar a hack**
menos ocho páginas web del gobierno peruano, según informó la Dire
(Dirincri).

"Estamos coordinando nuestra investigación y pidiendo información al FBI
hackers", dijo el coronel Oscar Gonzales, jefe de la División de Alta Tecnología

Gonzales señaló que el jueves **al menos ocho páginas del gobierno perua**
grupo que se hace llamar "Piratas de la Red" y que colgó en su página
páginas gubernamentales.

GRUPO NUEVO

Entre **las páginas que fueron atacadas están las de los Ministerios de**
Nacional Penitenciario y el servicio de Guardacostas.

"Este es un ataque de mayor nivel, no podemos precisar de dónde viene, pe
alojando la información hurtada esta fuera del país", indicó.

El **oficial descartó que Anonymous,** grupo hacker que ha atacado o a
gubernamentales de varios países. **esté detrás de esta acción** que por pri

Tras el arresto de tres supuestos miembros del grupo **Anonymous** en **España**, el mencionado grupo de **hackers** tomó represalias contra el sitio Web de la **policía española** y lo **hackeó.**

De esta forma, los **hackers** atacaron el sitio **www.policia.es** y lo dejaron sin acceso a la red durante una hora, el día de ayer 12 de Junio desde las 21:30 GMT.

Las autoridades **españolas** no han podido confirmar que se trate efectivamente del grupo **Anonymous**, pues sólo indicaron que el sitio se había caído por una hora. A pesar de esto, se colocó un anuncio en un sitio relacionado a **Anonymous**, donde los miembros del grupo se adjudicaron el ataque, el cual llamaron **#OpPolicia.**

Según informaciones del grupo, se habría utilizado un ataque distribuído de denegación de servicio (**DDoS**). Este tipo

Otros “Casos de Éxito”

Adhiérase

Si es usted una empresa o un organismo público y quiere adherirse a Confianza Online, nosotros le informamos cómo conseguirlo:

Infórmese Aquí

Preguntas Frecuentes

Histórico de Noticias

CONFIANZA ONLINE
AGENTE OFICIAL

Agentes Oficiales de Confianza Online

adigital

AUTOCONTROL

Que confianza Online pueden OFRECER cuando ellos no son ni seguros.

Noticias Confianza

1º “extracto” UNA DE LAS
de Tecnologías de la Comun
100% por red.es. Su objetiv
proyectos relacionados con
digital y así como solucione
de León.):

AVISO AL INTECO Y SUS J

http://www.youtube.com/wa

Este es un mensaje anónimo
a todo el mundo, todo el tie
acallar la libertad de expres
completamente inútiles. Cua
exigencias, más expuestos
criminal de una pequeña eli
que se les exige. Cuanta má
su propia autoridad. Por cad
o publican, crecen cientos d
ha evolucionado. Ahora som
tecnología, compartiendo in
alienarnos ya no serán efec
desgaste a la vista de todos
sonrisa forzada y continúan
decadente monarquía parlar
despierta, no puede sino int
combatir, que no puede sile
una discordia que les favore
continúa adelante y el mens
una muestra patente de la i
que no nos representa ni tra
acampadas de grupos o per
rebelión ciudadana, nadie ha

LulzSec hackeó la web de la presidencia de Brasil

Posteado por: **identidadesenpeligro** | junio 22, 2011

El grupo LulzSec parece no tener paz y esta vez le tocó a Brasil. La web del gobierno y de la presidencia de Brasil fueron hackeadas durante la madrugada de este miércoles por el grupo de piratas informáticos LulzSecBrasil. El grupo internacional LulzSec felicitó a sus compañeros.

Tanto la web de la presidencia (www.presidencia.gov.br) como del gobierno brasilero (www.brasil.gov.br) quedaron fuera de servicio luego de un ataque informático del que también fueron víctimas hace pocos días organismos estadounidenses.

LulzSecBrasil, el sector brasilero de los hackers LulzSec, se responsabilizó por lo ocurrido y afirmó vía Twitter: “Es hora de mostrar a los gobiernos corruptos del mundo que ellos no tienen derecho a censurar, no importa tu color de piel, origen, o creencia, nosotros te convidamos a sumarte a nosotros”.

El grupo internacional LulzSec agradeció a LulzSecBrasil vía Twitter y aseguró: “nuestra unidad brasileña está progresando, bien hecho hermanos de @LulzSecBrasil”.

Ambos sitios fueron restablecidos y se encuentran funcionando con normalidad.

Escrito por Identidades en Peligro

comisión. Los cambios exigidos por el pueblo son mas que claros: Democracia participativa. Reforma de la ley electoral. Separación de poderes real. Absoluta transparencia política y fiscal. Ferreo control sobre bancos y corporaciones. Aún siendo solo un comienzo, dichos cambios ya son mucho mejores

Requisitos Legales

La Normativa sobre Seguridad de la Información en el Estado Uruguayo

Legislación Aplicable

- Ley de Habeas Data y Protección de Datos Personales - 18331
  - Proceso de Habeas Data
  - Protección de los datos personales almacenados
  - Registro de Bases
  - Consentimiento Informado..
- Ley de Acceso a la Información Pública - 18381
  - Establecer procedimiento para la Clasificación de la información
  - Publicar información Pública.

- Existen diferentes casos en los que surgen conflictos entre ambas leyes.

Legislación Aplicable

- Decreto de Política de Seguridad de la Información
  - Designación de un Responsable de la Seguridad de la Información.
  - Designación de un Comité de Seguridad de la Información.
  - Implementación de un Sistema de Gestión de la Seguridad
- Resolución AGESIC de Políticas de Gestión de Riesgos y Gestión de Incidentes de Seguridad.
  - Formalizar Metodología de Gestión de Riesgos.
  - Divulgar el análisis de riesgos a los actores involucrados.
  - Establecer planes de tratamiento.
  - Formalizar un proceso y procedimiento de gestión de incidentes de seguridad.

El Proceso

La Implementación gradual de un Sistema de Gestión de la Seguridad de la Información.

El sistema de gestión de la seguridad de la información (SGSI) es la parte del sistema de gestión del organismo, basado en un enfoque de riesgos, para:

establecer, implementar, operar, monitorear, mantener y mejorar la seguridad de la información.

¿Seguridad de la Información?

- La seguridad de la información consiste en procesos y controles diseñados para proteger información de su divulgación no autorizada, transferencia, modificación o destrucción, a los efectos de:
  - asegurar la continuidad del negocio;
  - minimizar posibles daños al negocio;
  - maximizar oportunidades de negocios.”

- *La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada.*

- La información puede estar:
  - **Impresa o escrita en papel.**
  - **Almacenada electrónicamente.**
  - **Trasmitida por correo o medios electrónicos**
  - **Mostrada en filmes.**
  - **Hablada en conversación.**

(Planificar /Hacer /Verificar /Actuar)

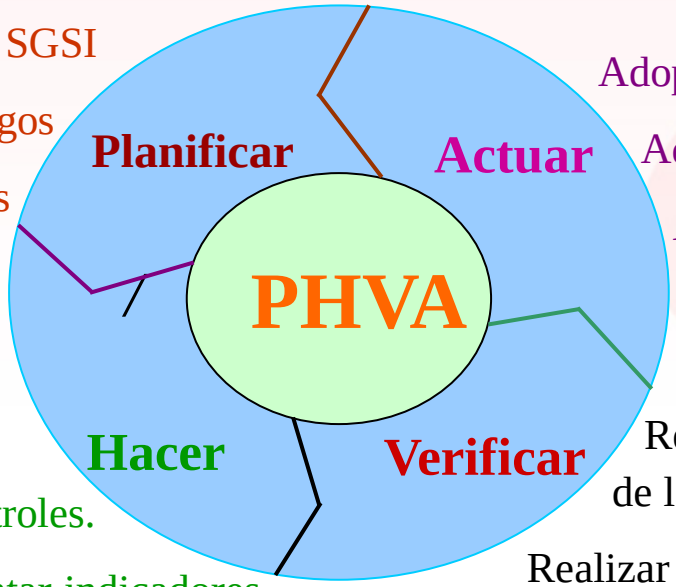
- Detalle de la metodología de la ISO/IEC 27001

Definir la política de seguridad

Establecer el alcance del SGSI

Realizar los análisis de riesgos

Seleccionar los controles



Adoptar acciones correctivas

Adoptar acciones preventivas

Adoptar acciones de mejora

Implantar el plan de tratamiento

Implantar el SGSI

Implantar los controles.

Implantar indicadores.

Revisiones del SGSI por parte de la Dirección.

Realizar auditorías internas del SGSI

Revisar la eficacia de los controles

¿Que tan seguros?

- **Existen tres fuentes principales para identificar el nivel de seguridad que debemos lograr:**
- *La primer fuente procede del Análisis de los riesgos a los que se ve expuesta la información de la organización.*
- *La segunda fuente es el conjunto de requisitos legales, estatutarios, reglamentarios y contractuales que debe satisfacer la organización.*
- *La tercera fuente está formada por los principios, objetivos y requisitos que la Organización ha desarrollado para apoyar sus operaciones.*

El SGSI en la organización

Se debe iniciar un proceso gradual, que implica un cambio cultural.

La seguridad de la información, y la de sus sistemas de procesamiento, debe ser un prioridad, y parte fundamental de la responsabilidad social de las organizaciones.

Primeras Tareas a Realizar

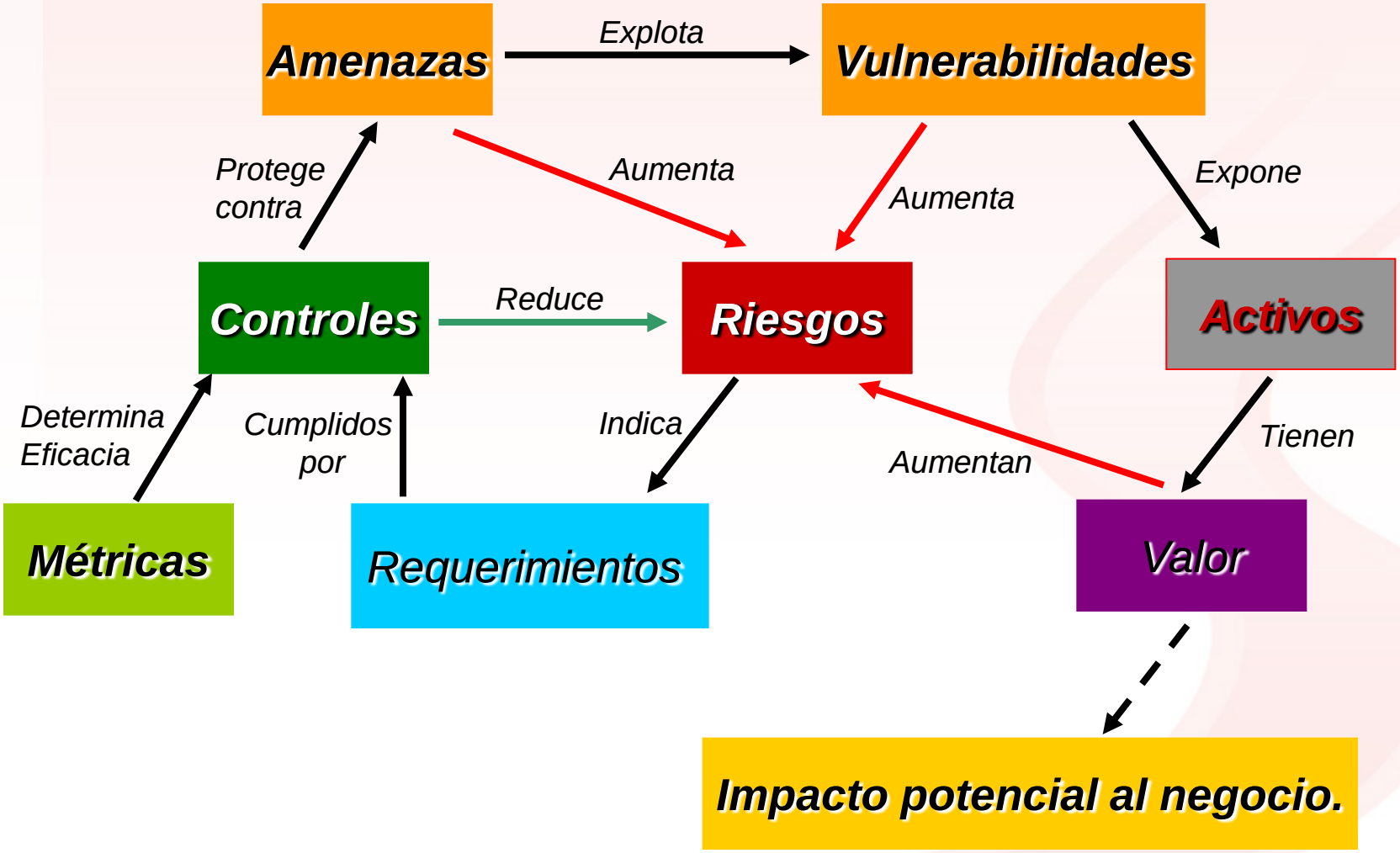
- Establecer el marco Organizacional para la Gestión de la Seguridad de la Información.
  - Designar y apoderar al Comité de Seguridad de la Información y
  - Responsable de Seguridad de la Información.
  - Establecer las responsabilidades de todos los actores involucrados.
- Establecer las bases del marco formal.
  - Resolución de Políticas de: Seguridad de la Información, Gestión de Riesgos y Gestión de Incidentes.
  - Establecer un Procedimiento y Herramienta para el Reporte de Incidentes de Seguridad.
  - Establecer un Plan de Capacitación y Concientización en Seguridad
- Realizar un primer Análisis de Riesgos de Seguridad en un alcance limitado.
- Establecer un Plan de Seguridad Anual.

El Responsable y Comité de Seguridad

- Responsable de Seguridad:
  - Lidera el proceso operativo.
  - Deben contar con el respaldo explicito y activo de la Dirección General.
  - Debe trabajar en coordinación con el Comité de Seguridad.
  - Debe priorizar el mantener un proceso gradual, firme.
  - Debe saber difundir la Gestión de Riesgos a todos los actores.
  - Debe gestionar el proceso de gestión de Incidentes.

- El Comité de Seguridad
  - Deben contar con el respaldo explicito y activo de la Dirección General.
  - Debe analizar las políticas y procedimientos a presentar a la dirección.
  - Debe lograr consensos e impulsar el proceso de cambios..
  - Debe sesionar de forma periódica (bimensual, etc.)

Gestión de Riesgos - Fundamentos



El Plan de Tratamiento

La implementación de controles técnicos y físicos en ausencia de un proceso de gestión formal lleva gradualmente a su ineficacia.

Objetivos de Control y Controles

Edición 2005		Objetivos de Control	Controles
5	Política de Seguridad	1	**2**
6	Aspectos organizativos para la seguridad	2	**11**
7	Gestión de los activos	2	**5**
8	Seguridad de los Recursos Humanos	3	**9**
9	Seguridad física y del entorno	2	**13**
10	Gestión de comunicaciones y operaciones	10	**32**
11	Control de accesos	7	**25**
12	Adquisición, Desarrollo y mantenimiento de sistemas	6	**16**
13	Gestión de incidentes de seguridad de la información.	2	**5**
14	Gestión de continuidad del negocio	1	**5**
15	Conformidad	3	**10**
Totales		**39**	**133**

Ej. Plan de Seguridad de la Información

- Entre los principales controles y tareas a realizar que se han identificado de importancia se encuentran:
  - Respaldo al Comité y al Responsable de Seguridad por parte de la Dirección.
  - Formalización de Políticas y Procedimientos para el control de acceso físico, incorporación/egreso de RRHH .
  - Formalización de Políticas y Procedimientos para el control de acceso lógico a sistemas/aplicaciones y documentación.
  - Formalización de un Plan para la continuidad Operativa.
  - Formalización de Procedimientos para el cumplimiento con la Ley de Acceso a la Información Pública.
  - Capacitación y Concientización del Personal
  - Implementación de controles técnicos y físicos para la implementación de las políticas y procedimientos definidos.

Buenas Prácticas – Ej. de controles

- Seguridad de los RRHH.
  - Los ingresos/egresos de RRHH (funcionarios, pasantes, contratos, etc.) debe requerir un proceso formal de comunicación a todas la partes involucradas en la gestión de la seguridad (física, lógica, etc.)
  - Se deben destacar y capacitar/concientizar a los RRHH de sus derechos y obligaciones en relación a la seguridad de la información, y el cumplimiento de las políticas y procedimientos establecidos.
  - En los casos que corresponda se deben establecer relaciones contractuales, que permanecen luego de finalizada la relación, con respecto a la Confidencialidad de la Información que manejamos.

Buenas Prácticas – Ej. de controles

- Seguridad Física y ambiental
  - El ingreso a las áreas seguras (Ej. Datacenter, Archivo) debe ser estrictamente restringido al personal autorizado.
  - Todo tercero debería ser identificado y registrado antes de acceder a sectores restringidos para funcionarios.

- Continuidad del Negocio.
  - Debemos contar con un plan y una estrategia implementada para garantizar la continuidad de los procesos críticos ante incidentes de seguridad, desastres, etc.

El Plan de Tratamiento en Nuestro Escritorio


FORECASTS
M&A ACTIVITY
THESAURUS
PROJECT CODENAME: YARMOUTH
F/MERGERS/TARGETS
P/Ns EXECD
TARGET DATES:
Architecture


FORECASTS
M&A ACTIVITY
THESAURUS
PROJECT CODENAME: YARMOUTH
F/MERGERS/TARGETS
TARGET DATES:
Architecture
20
11
16
2
13
5
7
14
9
3
10
8
4
1
19
18
12
17
6

Factores críticos de éxito

´ El apoyo visible y el compromiso evidente de la alta dirección ´

Factores críticos de éxito

- GESTION DEL CAMBIO:

Es fundamental comprender que es necesario un cambio en la forma de trabajo, y como tal siempre genera turbulencias dentro de la organización, que deben ser analizadas y tratadas.

De lo contrario, tal vez el proyecto de implantación sea exitoso, pero difícilmente su mantenimiento lo sea. Finalmente, no aportará el valor deseado.

Factores críticos de éxito

- El apoyo visible y el compromiso evidente de la alta dirección
  - Comprensión de los objetivos sus responsabilidades.
  - Asignación de recursos económicos y en especial humanos.
  - **Concientización de los mandos medios y de todo el personal.**
  - **Respaldo al Comité y Responsable de Seguridad**
- Un alcance, política y objetivos que reflejen los objetivos de la Organización.
  - Alinear los Objetivos de Seguridad con los Objetivos Estratégicos.
  - Comenzar por un alcance limitado
- La gestión de riesgos como elementos fundamental.

Factores críticos de éxito

- La adecuada capacitación y permanente concientización del personal.
  - Un plan permanente de capacitación y concientización en la materia.

- Un sistema de gestión de incidentes que permita centralizar el registro y seguimiento de los eventos e incidentes de seguridad.

- Reconocer que se trata de un proceso gradual, pero con metas claras.

Factores críticos de éxito (Segunda Fase)

- Un sistema integrado de indicadores que permita evaluar la eficacia de los controles y procesos implementados.

- Herramientas de gestión de permita centralizar el registro y seguimiento de diferentes procesos y controles.

- Herramientas de gestión de la documentación y los registros.

Factores críticos de éxito

Para finalizar

La necesidad de un cambio cultural.

Cambio Cultural

- Ej. Seguridad Vial.
  - El primer cinturón de seguridad fue incluido en autos FORD en 1956.

- No basta con implementar controles. Debemos velar por su continuo cumplimiento, junto al análisis y mejora de su eficacia.

- El cumplimiento de buenas prácticas en materia de seguridad es un elemento a incluir en el día a día, dentro y fuera del lugar de trabajo, para nuestro propio beneficio.

Datasec

Datasec
IT Security & Control

No es un tema más, es nuestra pasión!

Consultas

Javier@datasec-soft.com
Reynaldo@datasec-soft.com

ISO 27001 (IS 543115)