Gestión efectiva del riesgo de la información-buenas prácticas con base a COBIT 5 e ISO 27001


Bienvenidos

René Humberto Rodríguez Mejía

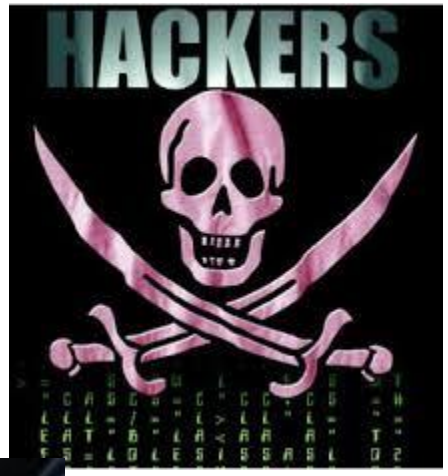
¿Por qué debería atender el riesgo de información?

¿Qué controles debería establecer?


DES
CONFIANZA

Principales delitos cibernéticos y de información

- Phishing
- Pharming
- Malware
- Usurpación de identidad
- Robo de información
- Manipulación no autorizada de información
- Clonación de tarjetas
- Pornografía infantil
- …



Casos en El Salvador

PRUEBAS DESDE EUA REVELAN CIBERATAQUE A LOS MEDIOS

JUDICIAL

El Salvador / Judicial

MÁS DE SUBSECCIÓN

- PNC incumple arresto domiciliar para contador de Grupo Samix, según defensa
- Matan a dos mujeres en Talnique y San Juan Opico
- PNC no pudo detener delincuentes que acababan de asaltar clientes de negocio de comida
- Operativo policial deja 21 capturados por estos delitos
- PNC: exministro de Salud contactaba a menores por medio de una tratante

Anonymous 'hackea' páginas web del Gobierno de El Salvador

Publicado: 7 nov 2011 22:13 GMT

El grupo de piratas informáticos Anonymous lanzó una serie de ataques contra páginas gubernamentales de El Salvador, lo que obligó al cierre temporal por seguridad de los sitios.

Anonymous 'hackea' páginas web del Gobierno de El Salvador / RT / AFP

EL DELITO QUE NADIE PERSIGUE

Región. Medios guatemaltecos reportaron en julio de 2014 que en promedio surgían a diario cinco casos de clonación, sumando para esa fecha 1,650.

La Unidad de Delitos Financieros de la PNC registra siete casos de clonación de tarjetas de crédito en todo 2015, una cifra que parece prometedora a primera vista, pero que en realidad solo refleja un subregistro por falta de denuncias, tanto por parte de los bancos como por parte de los usuarios. Por su parte, tampoco las autoridades fomentan la denuncia de delitos que se mantienen en la impunidad y continúan ocurriendo.

Y cada día son más y fáciles de realizar

Impulsores para implementar un SGSI

Pérdida de confianza

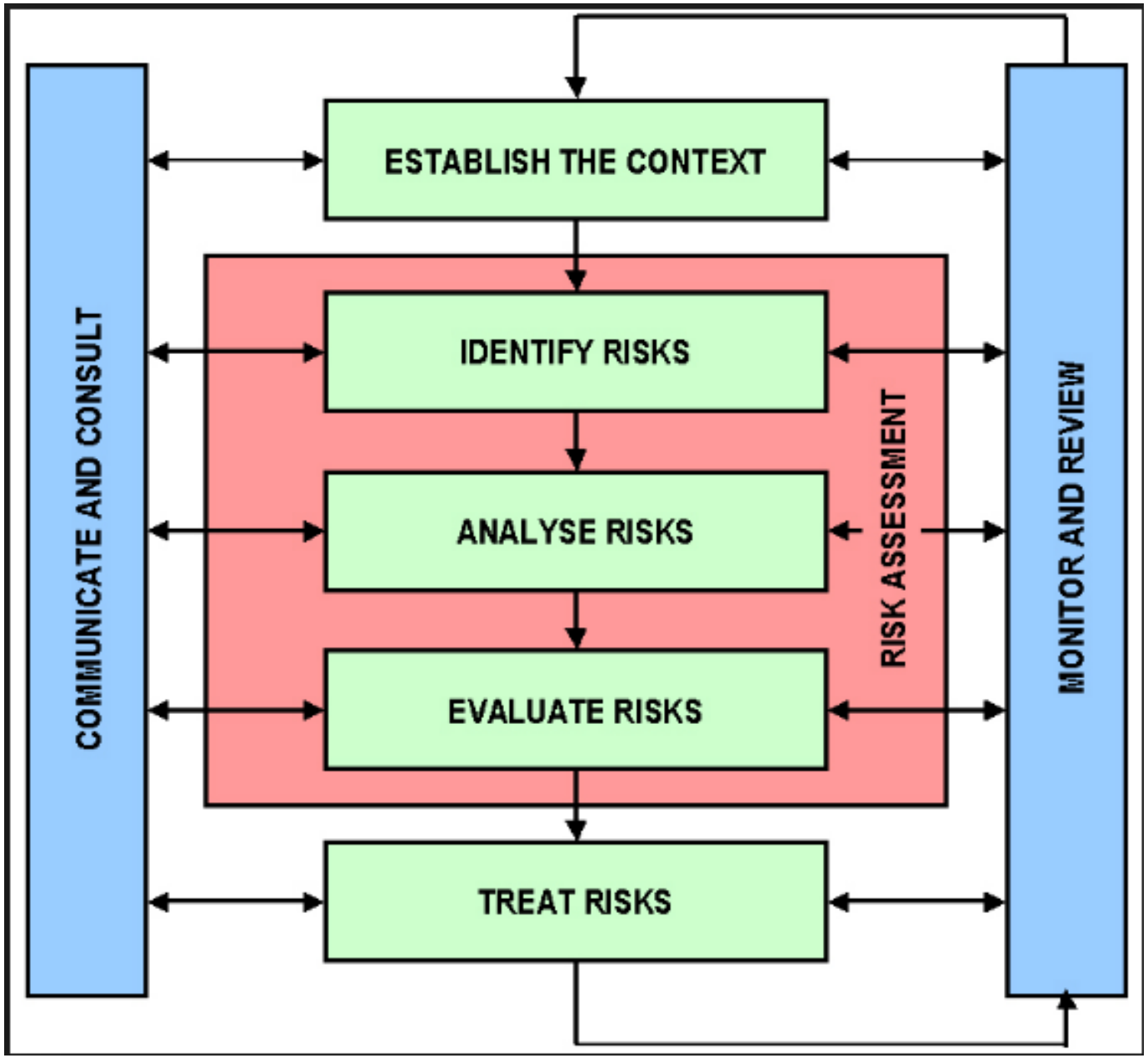
Conceptos básicos de seguridad de la Información

Conceptos básicos de seguridad de la Información

Controles mínimos para montar un efectivo SGSI

Primero- Análisis de amenazas y riesgos

Preparado por René Rodríguez-MBA, CISM



Fuente: COBIT-ISACA

Identificar contexto

Evaluación de riesgos

Atender el riesgo y monitorizar

Segundo- Alinearse con las necesidades del negocio/organización

Importante- Apoyo de la Gerencia General

Negocio	Seguridad
Ventas	Reputación
Ganancia	Cuidar al cliente
Ingresos	Evitar pérdida

¿Cómo se logra el apoyo de la Gerencia?

SGSI

Objetivos de negocios

Mismo rumbo

Análisis costo beneficio

Objetivos de negocios

Pretende determinar la conveniencia de un proyecto mediante la valoración en términos monetarios de todos los beneficios y costos derivados directa e indirectamente de dicho proyecto.

Este método se aplica a obras sociales, proyectos colectivos o individuales, empresas privadas, planes de negocios..., prestando atención a la importancia y cuantificación de sus consecuencias sociales y/o económicas.

Mismo rumbo

Tercero- Política de Seguridad de la Información

Política del SGSI

Clasificación de la información y etiquetado de documentos	Administración interna y externa de información	Seguridad equipos de TI
Protección de equipos informáticos usuario final	Administración de accesos	Controles de entrada y salida de personal
Seguridad en aplicaciones	Sistemas de negocios electrónicos	Seguridad de infraestructura informática
Conexiones a Internet	Administración de incidentes	Continuidad de negocios

Cuarto- Crear indicadores

Indicadores

Usuarios sin ingresar a red más de X días

Número de incidentes alertados

Cantidad de análisis a servidores

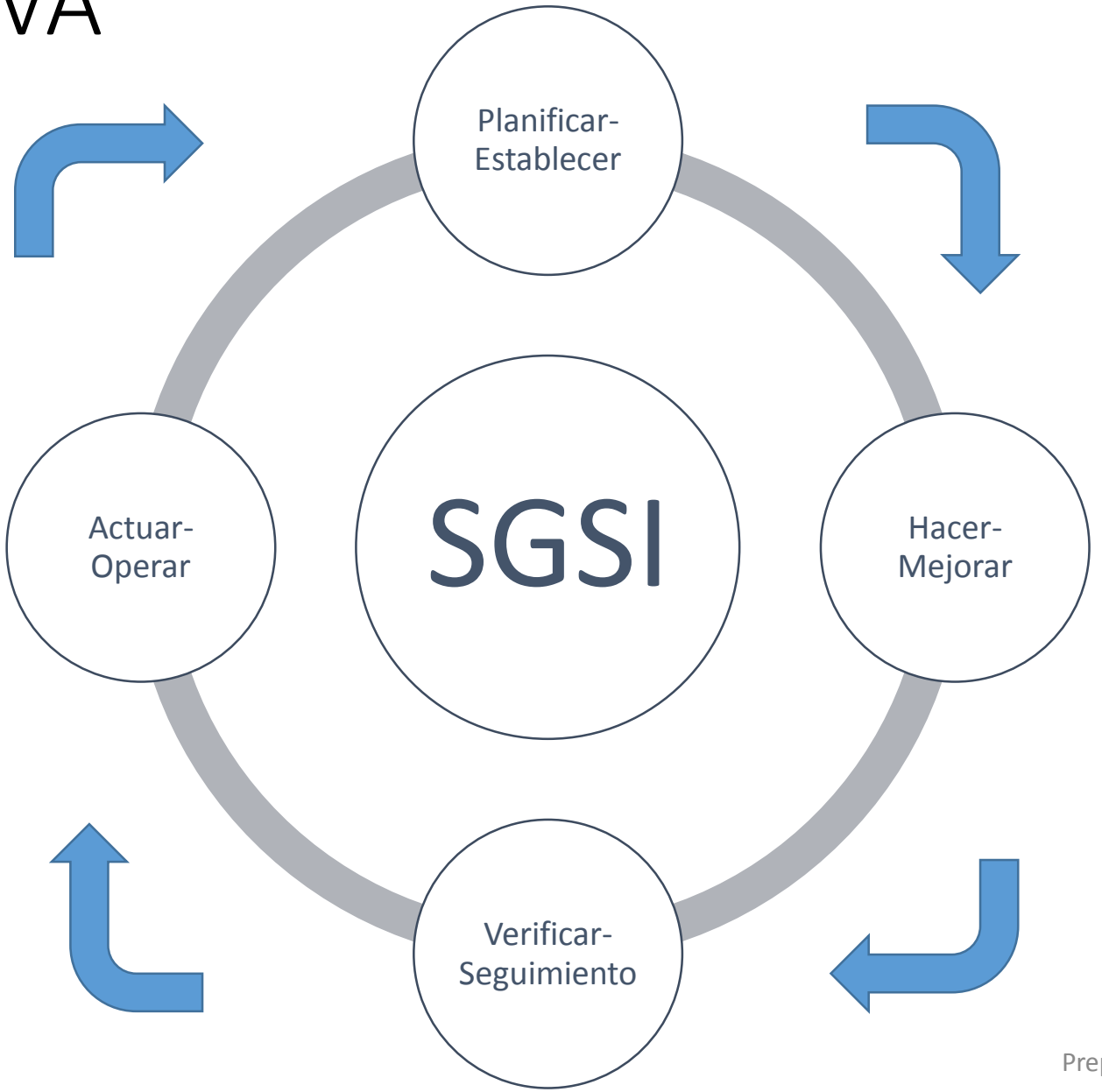
Proveedores clave revisados

Quinto- Asegurar mantenimiento

Modelo PHVA

Partes interesadas

Requisitos y expectativas del SGSI



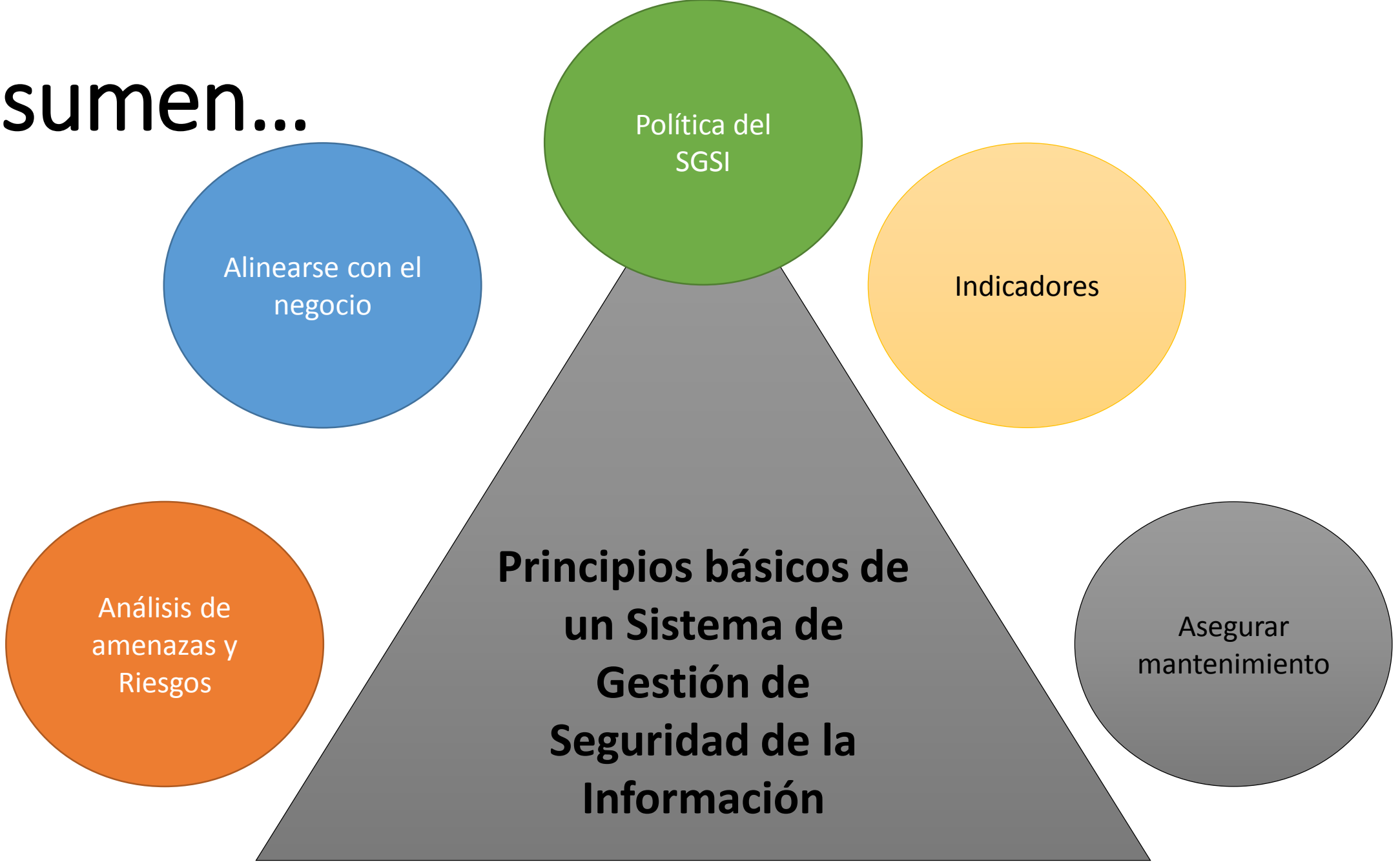
Partes interesadas

Seguridad de la Información gestionada

Modelo PHVA (PDCA en Inglés)

- ✓ **Plan (Establecer el SGSI):** Política SGSI, objetivos, procesos,procedimientos para la Administración de Riesgos y mejoras en la Seguridad Informática y resultados acordes a las políticas y objetivos de la organización.
- ✓ **Do (Implementar y Operar el SGSI):** Forma en que se opera e implementa la política, controles, procesos y procedimientos.
- ✓ **Check (Monitorizar y Revisar el SGSI):** Analizar y medir los proceso relacionados al SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.
- ✓ **Act (Mantener y Mejorar el SGSI):** Acciones preventivas y correctivas, basadas en auditorías internas y revisiones del SGSI.

En resumen…


Política del SGSI
Alinearse con el negocio
Indicadores
Análisis de amenazas y Riesgos
Asegurar mantenimiento
Principios básicos de un Sistema de Gestión de Seguridad de la Información

Comentarios… dudas

MAESTRÍAS UTEC

POSTGRADOS	Duración	Inicio	Horarios
Logística y Comercio Internacional	6 Meses	Sábado 02 de septiembre de 2017	Sábado de 8:00 a.m. a 12:00 p.m.
Mercadeo Estratégico Digital	6 Meses	Sábado 02 de septiembre de 2017	Sábado de 1:30 p.m. a 5:30 p.m.
Psicología Forense y Asistencia a Víctimas del Delito	6 Meses	Sábado 02 de septiembre de 2017	Sábado de 8:45 a.m. a 12:45 p.m.

SEMINARIOS	Duración	Inicio	Horarios
Seminario en Imagen y Marketing Personal, *Docente: Willie Maldonado*	8 Horas	Sábado 16 y 23 septiembre de 2017	Sábado de 8:00 a.m. a 12:00 p.m.
Uso de Dispositivos Móviles, Laptops y Desktops para Adultos Mayores *(con el apoyo de instructores en las clases)*	6 Semanas	Lunes 04 septiembre de 2017	Lunes y Miércoles 9:30 a.m. a 11:30 a.m.

Maestrías en: Administración de Negocios, Administración Financiera y Banca y Finanzas.

Inicio de clases: 02 de octubre.

Para mayor información: Tel.: 2275-2710 y 2711 correo: maestrías@utec.edu.sv Visite: www.utec.edu.sv/maestrías

MAESTRÍAS UTEC

René Humberto Rodríguez Mejía
Asesoría Gerencial
Consultoría en SGSI-Sistema Gestión Seguridad de Información
rerome3004@hotmail.com
Cel 7797 9534


Muchas
Gracias!