



SEGURINFO 2007

Tercer Congreso Argentino de la Seguridad de la Información

“Con la Seguridad en Mente”

Hotel Sheraton Buenos Aires - 15 de marzo de 2007

7 Claves para el Éxito de un Plan de Concientización en Seguridad de la Información

Santiago Cavanna

ISSA Argentina : www.ISSAArBA.org



Agenda

- ◆ Introducción
- ◆ 7 pasos para la construcción de un plan exitoso
- ◆ Suposiciones de contexto
- ◆ Análisis del problema del problema
- ◆ La persona en el centro
- ◆ Recomendaciones
- ◆ Métricos
- ◆ Referencias

Introducción

introducción

- ◆ No existe el plan perfecto, porque no existen organizaciones perfectas.
- ◆ Existen planes que se crean a partir de la cultura de una organización, opera sobre ella y la transforma.
- ◆ Es una tarea difícil, pero posible y con un alto impacto a mediano y largo plazo.

Definiciones

- ◆ Un plan de Concientización en seguridad de la información es diseñado para modificar conductas o reforzar buenas practicas de seguridad de la información.(*)
- ◆ No es una capacitación, pero esta estrechamente vinculada a ellas (anexos)
 - Concientización Responde el “Qué? (conciencia de riesgos y responsabilidades)”
 - Las capacitaciones responden el “Cómo? (prevención y respuesta frente a incidentes)”

7 pasos para la construcción de un plan exitoso

Concientización – capacitación – entrenamiento.



Pasos del Programa de Concientización en Seguridad

Fase1: Definición del alcance y programa

- Paso 1.1: Obtener información de antecedentes
- Paso 1.2: Evaluar las necesidades y el contenido
- Paso 1.3: Definir las campañas
- Paso 1.4: Elegir los métodos y los medios
- Paso 1.5: Crear una identidad
- Paso 1.6: Formalizar del programa

Programa de Concientización En Seguridad

Campaña de Concientización
Campaña de Concientización
Campaña de Concientización
Campaña de Concientización

Fase2: Diseñando campañas

- Paso 2.1: Establecer objetivos de la campaña
- Paso 2.2: Seleccionar los constructores de la campaña y los entrenadores
- Paso 2.3: Definir el contenido
- Paso 2.4: Definir el presupuesto final de la campaña

seguridad

detallados
de prueba

es finales

Fase 5: Midiendo la efectividad

- Paso 5.1: Medición
- Paso 5.2: Evaluación de resultados

Campaña de Concienti
Campaña de Concienti
Campaña de Concienti
Campaña de Concienti

7 pasos para la construcción de un plan exitoso.

- ◆ 1- evaluación de necesidades (qué y por qué)
- ◆ 2- diseño de programa (cómo)
- ◆ 3- definición de alcances (a quienes y que temas)
- ◆ 4- desarrollo del material (ver 2)
- ◆ 5- comunicación y logística (ver 4)
- ◆ 6- ejecución del plan (ver 2,3,4 y 5)
- ◆ 7- evaluación/feedback y reevaluación de necesidades. (todo otra vez)

Suposiciones de contexto

Suposiciones de contexto

- ◆ Principios de seguridad: Confidencialidad, Integridad, Disponibilidad.
 - Derivados: autenticación, autorización, no repudio, auditoria, responsabilidad, privacidad
 - Opuestos de seguridad: Revelación, modificación, destrucción.
 - Para las principales organizaciones (F500-G100), la confidencialidad esta en el 3er puesto de importancia
 - Para muchas organizaciones – confidencialidad y concientización están estrechamente relacionados, pero aun así consideran que casi todo puede resolverse con tecnología.
- ◆ Pilares de la seguridad: Tecnología, Procesos, Personas.
 - Con una clara tendencia a la “tecnología” como respuesta a todos los males.

Suposiciones de contexto

- ◆ Las organizaciones cuentan con políticas de seguridad.
- ◆ Las organizaciones han implantado la política de seguridad a través de tecnología, procesos y personas.
- ◆ Las políticas de seguridad están vigentes, responden los intereses del negocio y son soportadas por los altos mandos de la organización.
- ◆ Junto a la política de seguridad se ha realizado un analisis de riesgo.
- ◆ El personal esta capacitado en las técnicas (herramientas y procesos) de protección de la información.

- ◆ Aun asi, las fallas de seguridad se producen cada dia.
- ◆ Aun asi, las fallas de seguridad no "hacen caer la torre"

Suposiciones de contexto

- ◆ 98%+ de las personas siguen las reglas, son responsables, hacen su trabajo y cuidan los activos (físicos y de información) de la organización a la que pertenecen o los emplea.
- ◆ Del 2% restante se pueden decir muchas cosas, pero raramente se pueden identificar del resto.

Del 2 % restante, una parte:

- ◆ El explorador
- ◆ El empleado disgustado
- ◆ El espia
- ◆ El terrorista
- ◆ El ladron
- ◆ El activista
- ◆ El hacker novato
- ◆ El hacker a sueldo
- ◆ El competidor
- ◆ Paises enemigos (*)
- ◆ Dinero.
 - Extorsion
 - Fraude
 - Problemas financieros
- ◆ Curiosidad
- ◆ Venganza
- ◆ Seguridad laboral
- ◆ Convicciones politicas
- ◆ Vandalismo
- ◆ Terrorismo
- ◆ Espionaje
- ◆ Guerra (*)

Del 2 % restante, la otra parte:

Indiferencia e ignorancia

Actitudes típicas de los usuarios (interrelacionadas entre si)

- Falta de comprensión de la naturaleza de la amenaza de seguridad
- No considerar estas amenazas importantes
- Recaer sobre otras personas para que asuman la responsabilidad por la seguridad
- Negar toda responsabilidad por la seguridad
- Considerar el tema demasiado técnico.

Análisis del problema del problema

Análisis del problema del problema

- ◆ Que creen que ocurre cuando ustedes entran a una oficina y dicen algo así como:
 - “No pueden confiar en su compañero, no pueden confiar en su correo, no pueden confiar en Internet, no pueden confiar ni en su jefe, ni en sus empleados”
 - “Todos estamos en peligro, hay gente mala afuera y adentro que esta conspirando contra nosotros, que quiere destruirnos y abusar de nuestra buena voluntad, robarnos y dejarnos en ridículo frente a la comunidad”

Análisis del problema del problema

- ◆ Las organizaciones establecen una expectativa de seguridad, basada en la cultura de la organización.
- ◆ La cultura de la organización es dinámica, pero conducir el cambio, es un desafío en si mismo.
- ◆ Los cambios culturales impuestos compulsivamente provocan resistencia (aunque todos entiendan los beneficios)
- ◆ Los cambios requeridos surgen del análisis y la observación de hechos cotidianos (escritorios, mesa de ayuda, reportes de incidentes, logs de navegación, inventario de software y contenido en los puestos de trabajo, entrevistas con los empleados, gerencia, recursos humanos, limpieza, etc)

Pregunte!

- ◆ Como atacaría usted a la organización
- ◆ Si usted no fuera una buena persona, podría sacar provecho de la confianza que le tienen?
- ◆ Que el lo que falla en la seguridad de esta organización?
- ◆ Usted siente que trabaja en un entorno seguro?
- ◆ Podría usted bordear los controles si quisiera?
- ◆ Que piensa sobre los hackers? Como cree que son? Porque cree que hacen lo que hacen?, como lo hacen?
- ◆ Cree usted que en esta organización podría haber hackers?
- ◆ Cree usted que cuenta con las herramientas necesarias para hacer su trabajo?
- ◆ Que piensa de su PC, sistemas, infraestructura, etc, desde el punto de vista de seguridad?

Observe!



No solo esta desordenada, es insegura!



La persona en el centro

La persona en el centro

- ◆ Las personas como individuos y como parte de grupos tiene comportamientos rutinarios.
- ◆ Cambiar el comportamiento típico de una persona o un grupo no es una tarea sencilla y lleva alta resistencia.
 - Las personas no necesariamente están allí porque les gusta, y es probable que hagan lo que hacen porque creen que esta bien así, o porque creen que no puede ser de otra manera.
 - Las personas llevan adelante un proceso de toma de decisión frente a cada tarea que realizan (es automático, mecánico*, intuitivo y rutinario)
- ◆ Las personas pueden cambiar su comportamiento, por las buenas o por las malas (pero por las malas, suele traer consecuencias no deseadas).

Cultura de la organización

- ◆ Las personas tienen a tomar porciones de datos para construir un juicio y realizar tareas.
- ◆ Lo que parece lógico para una persona, realmente lo es para esa persona, pero en función de la información y las reglas que ha tomado del entorno,
 - nuevas reglas, producirán diferentes resultados (no únicamente por hacerlas obligatorias, sino por incorporarlas al repertorio de reglas intuitivas en las que se basa una decisión particular).
- ◆ La definición de aceptable (riesgo) también es función de la formación de cada individuo y de cómo valora los activos que protege o lo conciente de las consecuencias de una falla en seguridad.

Cambio cultural



El Cambio cultural requiere ajustes de todo el sistema, además de políticas (reglas) normas y procedimientos.

Como toman sus decisiones las personas?

1. Distinguir entre decisión y resultado
2. Analizar cómo se toman las decisiones actualmente, y como se desvían estas de un modelo ideal-racional de toma de decisiones
3. Describir la heurística utilizada (reglas intuitivas) que ayudan en la toma de las decisiones, y cómo impactan estas en la calidad de las decisiones en términos de seguridad.
4. Examinar cómo se toman decisiones en casos inciertos y cómo se enfrenta el riesgo.

Entender el proceso de toma de decisiones

- ◆ Un buen resultado es un estado futuro que ha sido comparado favorablemente con otros posibles estados.
- ◆ Una buena decisión es una acción lógicamente consistente con las alternativas conocidas, la información con la que se cuenta y las preferencias que uno posee.
- ◆ La calidad de la decisión debe poder ser juzgada por la información y conocimiento disponible en el momento que fue tomada.

Los decisores estratégicos son actores racionales que maximizan los resultados, primero analizan la información disponible, luego analizan las alternativas en orden de tomar el mejor curso de acción.

Juicios heurísticos

◆ Regla de los cinco puntos oscilantes.

- Emocional, basado en la experiencia personal, dependiente del humor o el cansancio.
- Estimaciones de probabilidad basadas en hechos ocurridos.
 - ♦ Presume asociaciones posiblemente erróneas, por falta de información.
- Basado en estereotipos (por exceso o por defecto)
 - ♦ Insensible a las estadísticas.
 - ♦ Insensible a los ejemplos.
- Basados en puntos fijos, relativos a quien lo presenta, como lo presenta, la opinión personal sobre la persona, el caso u otros puntos arbitrarios sin fundamentos claros.
 - ♦ Sobre estimación, exceso de confianza.
 - ♦ Falta de objetividad.
- Desvío de la confirmación (2-4-6)
- Creencias irracionales persistentes. (religiosa, moral, social, política, etc.)

Concientización y toma de decisiones

- ◆ Las decisiones individuales y grupales afectan la seguridad de la información.
 - Hay técnicas para mejorar el proceso de toma de decisiones y deben ser parte de la capacitación anexa al plan de Concientización.
- ◆ La definición de reglas, no es suficiente,
 - La comprensión y la ejercitación del proceso de toma de decisiones relacionado con la seguridad deben ser incorporados a la cultura de la organización.

Recomendaciones

Primero piense en las personas

- ◆ Las personas necesitan el contacto, la interacción directa.
- ◆ Hable con la gente, antes de definir los objetivos, antes de diseñar el plan, durante la ejecución del plan y por supuesto luego de cada acción.
- ◆ El presupuesto debería contemplar en promedio por lo menos 8 horas al año de charlas de concientización en seguridad (páguese unos almuerzos!)
 - Evalúe quien es la persona indicada para llevar adelante esas charlas.

Criterios de segmentación

- ◆ El plan de Concientización debe presentar únicamente la información relevante para cada grupo.
- ◆ Criterios de segmentación:
 - Nivel actual de Concientización
 - ◆ Oficinas y escritorios cerrados
 - ◆ Estaciones de trabajo aseguradas
 - ◆ Información y medios de almacenamientos asegurados
 - ◆ Incidentes de seguridad registrados
 - Categoría de trabajo
 - ◆ Mandos altos
 - ◆ Mandos medios
 - ◆ Supervisores y jefaturas
 - ◆ Empleados
 - ◆ Otros
 - Función específica
 - ◆ Proveedores de servicios (administradores, soporte, mesa de ayuda, etc)
 - ◆ Dueños de información
 - ◆ Usuarios de información
 - Conocimiento en el procesamiento de información
 - Sistemas o tecnologías utilizadas
 - ◆ Windows, unix, Mac, Mainframe, Usuarios móviles.

Dar el ejemplo y grupos especiales.

- ◆ Parte del soporte de la alta gerencia esta en el ejemplo.
 - Primeros en recibir el programa y dar un feedback, inclusive antes de que el programa haya sido aprobado.
 - Grupo de riesgo
 - El resto de la organización, observa los hábitos y costumbres
 - Obtención de mayor soporte económico y de recursos humanos para implantar el plan al resto de la organización.
- ◆ El área de IT es el segundo área donde se requiere generación de conciencia, antes que el resto de la compañía.
- ◆ La mesa de ayuda, necesita ser concientizada y además contar y estar capacitados en los procedimientos y herramientas utilizados para dar respuesta a los incidentes.
- ◆ Recursos humanos debe ser concientizado, porque los empleados recurren formal o informalmente a ellos por consejo, ayuda o reclamo.

La “Tarea”

- ◆ Planifique grande, pero comience pequeño
- ◆ Las organizaciones adhieren a un plan de Concientización y capacitación, pero luego se resisten a proveer los recursos humanos y financieros.

Utilice los recursos que tiene a mano primero, muestre resultados y vaya por mas.

correo electrónico, intranet, pósters, sticks, lapiceras y workshops enfocados a grupos de alto riesgo.

Métricas

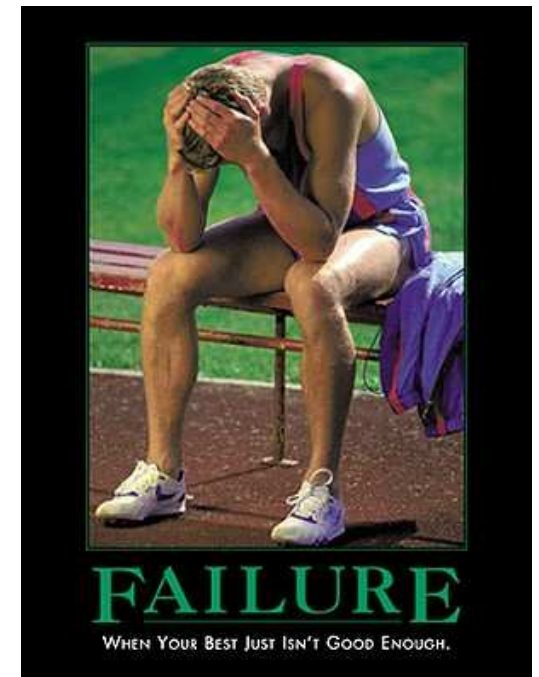
Métricas

- ◆ Las métricas son relativas y están relacionadas con los objetivos planteados.
- ◆ Pueden ser porcentuales o de percepción, pero deben ser establecidas, registradas e informadas.
- ◆ La retroalimentación es positiva, pero debe entender que los resultados pueden ser sorprendentemente diferentes a lo esperado.
 - Ejemplo: es habitual que los incidentes de seguridad aumenten dramáticamente luego de un plan ejecutado de Concientización de seguridad de la información.

Conclusión

Conclusión: Como comerse un elefante

- ◆ De a churrascos (lleva tiempo y paciencia)
- ◆ Comprenda la cultura de la organización
 - Comprenda que la organización (compuesta por individuos) se resistirá al cambio sistemáticamente.
- ◆ Defina la visión (establezca un gap)
- ◆ Cree un roadmap para implementar el cambio.
- ◆ No se desanime, Usted no es Superman y no se supone que esto ocurra silenciosamente durante la noche..



Referencias

- ◆ Agradecimiento a D.Glass (autor de algunos slides.)
- ◆ Jorge Coca (ISACA-ADACSI, autor de algunos slides)
- ◆ NIST (sp-800-50, sp-800-16)
- ◆ NoticeBorad
- ◆ SANS (sección de trabajos especiales)
- ◆ Lecturas complementarias.
 - Daniel Goleman – inteligencia emocional
 - Herve Fischer – CiberPrometeo
 - Malcolm Gladwell – Inteligencia Intuitiva
 - K Mitnick - Art of Deception



SEGURINFO 2007

Tercer Congreso Argentino de la Seguridad de la Información

“Con la Seguridad en Mente”

Hotel Sheraton Buenos Aires - 15 de marzo de 2007

Muchas gracias

Santiago Cavanna
scavanna@issaarba.org