EL ASPECTO HUMANO DE LA SEGURIDAD DE LA INFORMACIÓN: RESUMEN GENERAL

Rojas Valencia, Jorge Andrés
jorge-rojas1@upc.edu.co
Universidad Piloto de Colombia

Abstract **—**the security of information systems is not only a purely technical or documentary issue where only should matter policies, hardware and software, on the other hand there is a very important human factor that is usually neglected by professionals of information security as they are concentrated only in awareness. There are other areas in which intervenes humans, such as for example the use and interaction with these systems, for which we must pay special attention because as you will see the willingness of employees to comply with policies and therefore reducing the risk of occurrence of potential threats to information systems depends of them.

Resumen **—**la seguridad de los sistemas de información no es solamente una cuestión meramente técnica o documental en donde solo se deben considerar las políticas, el hardware y el software, por el contrario hay un factor humano muy importante que usualmente suele ser dejado de lado por los profesionales de la seguridad de la información ya que estos se concentran solo en la concientización. Existen otros ámbitos en los que interviene el ser humano, como lo son por ejemplo el uso y la interacción con estos sistemas, para los cuales debemos de prestar especial atención pues como verán de ellos dependerá la disposición de los empleados para el cumplimiento de las políticas y por ende la reducción del riesgo de ocurrencia de potenciales amenazas sobre los sistemas de información.

Índice de términos—Audiencia, Concientización, Interacción Humano Computadora, Seguridad de la información, Usabilidad.

I. INTRODUCCIÓN

La seguridad de la información como la imagina la mayoría de las personas hoy en día radicaría principalmente en complejos algoritmos de cifrado, firewalls, virus de computadora y habilidosas personas usualmente conocidas como hackers que se introducen y corrompen los sistemas sin autorización de sus propietarios. Sin embargo hay un aspecto de la seguridad de la información que la mayoría de las personas, relacionadas o no con el medio, desconocen o menosprecian, ese aspecto es el factor humano dentro de la seguridad de la información.

Usualmente relacionamos a las personas con la seguridad de la información desde una perspectiva ya sea del personal que necesita ser capacitado o bien sea como objetivos o vectores de ataque, sin embargo existen otro factor más que es importante tener en cuenta al momento de ver a las personas desde la perspectiva de la seguridad de la información y ese factor es el de la persona como usuario.

Recordemos que son las personas (usuarios) las que interactúan con los sistemas de información por medio de las interfaces que estos les proveen, por lo tanto el diseño de estas interfaces afectara la operación y percepción de los usuarios sobre los sistemas lo que finalmente afectara la disposición de estos para realizar un correcto uso de los sistemas y reduciría el riesgo de los incidentes de seguridad causados por el uso incorrecto del sistema.

II. INTERACCIÓN HUMANO-COMPUTADORA Y SEGURIDAD DE LA INFORMACIÓN

Para poder escribir acerca del aspecto humano de la seguridad de la información y conforme ha los que deseo expresar en este numeral, considero de gran importancia primero definir y aterrizar el concepto conocido como interacción humano computadora (HCI, human computer interaction).

Según la definición: "IHC (interacción hombre computadora) es el estudio de cómo las personas interactúan con las computadoras y en qué medida las computadoras están, o no están, desarrolladas para la interacción exitosa con los seres humanos" [1].

Podrán preguntarse ahora porque este concepto es relevante; para entender esta relación primero debemos recordar que los sistemas de información actúales son mucho más seguros y constantemente evolucionan para mejorar en este aspecto; sin embargo no importa que tan avanzada sea su seguridad estos son diseñados, creados, operados y trabajan para propósitos humanos. Es precisamente este último aspecto, la interacción e interfaz de estos sistemas con los humanos la que ha continuado generando en dichos sistemas avanzados las brechas de seguridad que encontramos hoy en día.

Pero porque pasa esto, pues como lo dice S.W. Smith en su publicación titulada *Humans in the Loop Human–Computer Interaction and Security*: "…estamos tratando de asegurar un sistema que encarna procesos humanos e incluye usuarios humanos, pero restringimos nuestro análisis y diseños a los computadores como tal…".

He allí el punto en donde se unen la IHC y la seguridad de la información, ya no es posible para los ingenieros y expertos de la seguridad de la información perfeccionar el desempeño en términos de seguridad de nuestros sistemas si no consideramos a los humanos y sus interacciones como un factor fundamental y decisivo a la hora de implementar y diseñar sistemas y controles de seguridad.

Finalmente deseo concluir con este segmento al incluir algunas frases y conclusiones de la publicación de S.W. Smith que fueron recogidas por este durante los distintos seminarios a los que este acudió:

- "Los hackers prestan más atención a la relación humana en la cadena de seguridad que incluso los diseñadores de seguridad".
- Los usuarios más jóvenes (que han crecido con las computadoras) perciben la seguridad como un obstáculo que tendrán que saltarse.
- Los sistemas tienen fallos de seguridad porque la configuración es demasiado difícil; incluso los usuarios con conocimiento no pueden entender algunas interfaces de usuario relevantes para la seguridad.

III. SEGURIDAD VS USABILIDAD

Quise incluir este segmento porque al fin y al cabo "la seguridad de cualquier sistema informático que está configurado y operado por los seres humanos depende fundamentalmente de la información transmitida por la interfaz de usuario, las decisiones de los usuarios de la computadora, y la interpretación de sus acciones" [5].

Para entender porque es importante pensar en el usuario y la usabilidad en el momento de diseñar las interfaces de los sistemas debemos comprender que las personas son seres con recursos y capacidades limitadas, las cuales generan adicionalmente modelos mentales del mundo que los rodea lo cual les facilita interactuar y comprender su entorno y los estímulos externos que reciben.

Primero miremos porque los recursos limitados de los seres humanos afectan la seguridad de los sistemas. Para entender esto solo tenemos que pensar en un día largo y estresante de trabajo en el cual las personas deben interactuar constantemente con diversos sistemas y en algunos casos tomar decisiones que quizás afecten no solo el desempeño sino también la seguridad los sistemas. Estas personas conforme avanza el día, o incluso la semana, se verán cada vez más agotadas (perdiendo recursos) y afanadas por terminar su trabajo y recuperar energías, perdiendo la capacidad de recordar y de tomar las decisiones adecuadas.

Por lo tanto entre más cansadas estén las personas, entre más complejo y largos sean los procesos con los que interactúan más apresuradas y poco certeras serán sus decisiones y en términos generales querrán saltarse todas las medidas y controles de seguridad (que impiden culminar rápidamente su trabajo). Consecuentemente, si durante el diseño y desarrollo de los sistemas pensamos en procesos e interfaces que faciliten y reduzcan el estrés y desgaste mental de las personas, estas podrán tomar mejores decisiones y no consideran a los controles de seguridad como medidas que entorpecen y alargan su trabajo.

Como punto final y para ejemplarizar el porqué los modelos mentales afectan la usabilidad debemos tener en cuenta que estos modelos ayudan a comprender y por lo tanto facilitar el uso de los sistemas de información y sus interfaces. En otras palabras reducir el tiempo y desgaste mental de las personas.

Un ejemplo claro de este punto está consignado en el libro de Leron Zinatullin en el cual se menciona el caso de la empresa Xerox y la introducción del escritorio grafico: "la gente era capaz de relacionarse con la interfaz gráfica de un ordenador en lugar de la línea de comandos. Podían manipular objetos de manera similar a como lo hacen con los escritorios físicos: almacenar y clasificar los archivos en carpetas, mover, renombrar o borrar al incluirlos en la papelera de reciclaje".

IV. CINCO MANERAS DE CONVERTIR A LOS EMPLEADOS EN ACTIVOS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS

Como se indico anteriormente la seguridad de los sistemas se ve afectada por la interacción de las personas con estos, por lo tanto los conocimientos de estas sobre la seguridad de la información son un valiosos punto a tener en cuenta para las compañías. A continuación podremos encontrar un conjunto de aspectos que pueden ayudarnos a convertir a los empleados en piezas claves para la protección de los datos de las compañías.

Antes de iniciar debo indicar que la información que está contenida en esta sección fue extraída del siguiente documento *Five Ways to Turn Employees into Security Assets for Protecting Data* de autoría de Glen Kosaka, en su momento director de productos DLP en Trend Micro [10].

A. Haga la seguridad de los datos parte de la cultura de su compañía

La protección de la información sensible no debe ser responsabilidad única de los equipos y ejecutivos de seguridad. Cada jefe de departamento tiene la responsabilidad de ayudar a identificar y localizar los datos sensibles, y proponer políticas para el acceso adecuado, además del uso y la protección de los datos por parte de los empleados. Cada empleado que ha sido identificado como poseedor de acceso a los datos sensibles debe someterse a entrenamiento en las políticas y procedimientos que

definen el cuidado responsable de los datos de la empresa. De esta manera, los empleados y directivos por igual comparten la responsabilidad de no sólo el uso de datos sensibles, pero también de servir para vigilar a los demás para asegurarse de que todo el mundo está siguiendo estas políticas.

B. Integrar procesos de prevención de fuga de información al flujo de trabajo general

Muchas empresas han perdido el control sobre sus datos sensibles debido a que la identificación, el acceso y la circulación de los datos sensibles no están integrados en sus procesos generales. Por ejemplo, cuando se crean nuevos documentos o contenidos, ¿existe un proceso de clasificación para determinar las políticas adecuadas que se deben aplicar? o cuando los empleados se unen a un departamento o son transferidos entre los departamentos se inician los procesos y controles de protección de datos y acceso de los servicios en los nuevos y anteriores departamentos. Además, la introducción de nuevos dispositivos móviles o sedes remotas de desarrollo puede introducir nuevos vectores de amenazas para las fugas de datos. Cuando las empresas piensan a través de sus procesos básicos e incorporan medidas de protección de datos según el caso el riesgo de fugas de datos se reduce significativamente.

C. Haga que los empleados se sientan como activos de seguridad, en lugar de pasivos

Si los empleados pueden sentirse como vigilantes sobre la protección de los datos de la empresa, así como lo hacen sobre el cumplimiento de otros objetivos de negocio, se convierten en un activo muy valioso para los programas de seguridad de datos de su empresa. Salvar a sus empresas de los millones de dólares en multas y gastos asociados con las brechas de seguridad puede ser tan valioso como el ahorro de la compañía al mejorar los procesos o al reducir los costos, por no hablar de la vergüenza y la pérdida de buena imagen asociada con violaciones a la privacidad. Los programas de formación y sensibilización en torno a los costos de los diversos tipos de brechas y de lo que los empleados pueden hacer para prevenir las brechas sensibilizaran a estos de cara a los desafíos que enfrentan.

D. Prevenir la tentación de verse implicado la violación inofensiva de políticas

Si bien hay muchos obvios "no-no", tales como la venta de la lista de cuentas de la compañía a un competidor, también hay muchas violaciones de "zona gris", que, si se deja sin tratar, puede provocar brechas más dañinas. Estos incluyen compartir listas de contactos con amigos en otras empresas, generar copias de respaldo de los datos sensibles en los sistemas caseros o dispositivos de almacenamiento no autorizados y la copia de propiedad intelectual a las memorias USB para transportarlos a un sitio de desarrollo remoto. Todas estas violaciones, si bien pueden parecer inofensivas a los empleados que las cometen, pueden dar lugar a infracciones costosas.

Además, mientras a los empleados se les permita ampliar los límites de lo que pueden hacer y salirse con la suya, puede aumentarse la tentación de sacar provecho de estas violaciones. Si bien hay muchas alternativas para la supervisión y aplicación de las políticas, los criterios de selección de un programa de prevención de fuga de datos (DLP) deben incluir la inteligencia suficiente para detectar fugas relevantes sin molestar a los empleados y afectar al negocio y la productividad.

E. Enseñar a los empleados acerca de las políticas, mientras que hacerlas cumplir

Una política de seguridad de los datos eficaz debe incorporar un enfoque de "un palo y la zanahoria". Los empleados deben ser educados acerca de las políticas de la empresa, de ser posible en el "punto de uso" o "punto de violación." Cuando un empleado crea copias de un documento sensible en una unidad USB violando las políticas, es el mejor momento para educarlos sobre la protección adecuada de los activos valiosos de la compañía. Si las violación es grave la acción debe ser bloqueada por la solución DLP, y el superior del empleado debe ser notificado, así se pueden tomar medidas adecuadas. Incrementado la sensibilización de los empleados acerca de las políticas de protección de datos, especialmente en el "punto de uso", puede reducir o incluso eliminar el gran porcentaje de las infracciones que se producen por accidente y sin querer.

La tecnología de prevención de pérdida de datos no sólo debe controlar y prevenir las fugas, sino también ayudar a educar y sensibilizar a los empleados sobre las políticas y procedimientos para el manejo de datos sensibles de la compañía. Al educar a los empleados y salvaguardar tanto el perímetro de la red como también los puntos finales internos, las soluciones de DLP también pueden ayudar a que los empleados se conviertan en activos de seguridad mediante la prevención de fugas de datos, lo que reduce las infracciones accidentales y requiriendo su vigilancia para proteger los datos sensibles.

Sin embargo, cualquier nueva tecnología que afecta las actividades diarias de los empleados debe ser inteligente y precisa para evitar la reducción de la productividad y la creación de frustración de estos. Una fina línea debe ser trazada entre la vigilancia y aplicación de las políticas de prevención de fugas de datos críticos y la permisividad que permita a los administradores hacer su trabajo y mantener el negocio en crecimiento.

V. CONOCIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

La mayoría de las organizaciones hoy en día apoyan sus procesos productivos en sistemas de la información los

cuales pueden llegar a contener, manipular o administrar datos sensibles de la compañía. Cuando dichos sistemas y datos son comprometidos y se ven afectados por una falla en la seguridad, a menudo tienen graves consecuencias financieras y de reputación para las empresas y sus clientes.

Teniendo en cuenta que dichos sistemas son manipulados por los usuarios (recuerdan el titulo anterior IHC), internos y externos de las compañías, y que estos a menudo son considerados el eslabón más débil en la seguridad de la información, podríamos deducir que entre mejor preparados y mayor conocimiento acerca de la seguridad de la información posean dichos usuarios menor será la probabilidad de ocurrencia de una falla de la seguridad de la información a causa de dichos empleados.

Por ejemplo, una de las fuentes citadas [2] indica que entre el 50 - 70% de los incidentes de los sistemas de seguridad de la información en las organizaciones se dan como resultado, directa o indirectamente, por el mal uso de los empleados, ubicando estos desde errores de ingenuidad a daños intencionales.

Pero entonces que se puede definir como conocimiento de la seguridad de la información. De nuevo durante la lectura y búsqueda de las diversas fuentes de información consultada encontré que la mayor parte de estas siempre discutió acerca del conocimiento de la seguridad de la información (ISA, information security awareness como se conoce en ingles) desde un punto de vista corporativo, y como se relaciona esta con el cumplimiento o el deseo de cumplir con las políticas de seguridad de las compañías en las que los empleados se desempeñan.

Quizás por esa remarcada inclinación a relacionar este concepto a contextos empresariales, dejando de lado el contexto de la persona fuera de las corporaciones, me pareció como la definición más acertada la siguiente ya que incluye un factor fuera de lo laboral en la definición: "comprensión general de un empleado acerca de la seguridad de la información y su conocimiento de las políticas de seguridad de la información de su organización" [4].

Siguiendo con esta línea de definición y extraído de la misma fuente:

- Comprensión general de seguridad de la información se define como el conocimiento y comprensión general de un empleado de los problemas potenciales relacionados con la seguridad de la información y sus ramificaciones.
- Conocimiento de las políticas de seguridad se podría definir como el conocimiento y entendimiento de los requerimientos prescritos en las políticas de seguridad de la información de la organización y el objetivo de estas.

Entonces tenemos que todo empleado en toda compañía tiene estos dos componentes partes de su conocimiento en seguridad de la información, por lo tanto (a pesar de que como se dijo anteriormente los empleados son el eslabón más débil) potenciando el conocimiento de estos, ellos también pueden ser grandes activos en el esfuerzo para reducir el riesgo relacionado con la seguridad de la información.

Este será el tema del siguiente segmento, como convertir a estos empleados en activos de seguridad para proteger la información.

VI. LISTA DE VERIFICACIÓN PARA UN PROGRAMA DE CONCIENTIZACIÓN DE SEGURIDAD

A continuación incluyo una lista de verificación que puede ser usada como apoyo al momento de planificar y administrar programa de concientización en seguridad de la información. Este listado, nos dará una guía del que debemos tener en cuenta y posteriormente en las siguientes secciones hay una explicación más detallada de algunos de estos puntos. Esta lista de verificación puede ser hallada en el documento del PCI publicado con el siguiente nombre *Best Practices for Implementing a Security Awareness Program* [11].

A. Creando el programa de concientización sobre seguridad

1) Identifique los estándares de cumplimiento o auditorio a los que su organización se debe ceñir.
2) Identifique los conocimientos requeridos para aquellos estándares.
3) Identifique los objetivos, riesgos y políticas de seguridad de la organización.
4) Identifique los interesados y consiga su apoyo.
5) Cree una línea base para el conocimiento de seguridad de la información.
6) Cree el mapa del proyecto para establecer el alcance del programa de formación de conocimiento de seguridad.
7) Cree el comité de guía que asista en la planeación, ejecución y mantenimiento del programa de concientización de seguridad.
8) Identifique a quien va a tener de objetivo-roles diferentes pueden requerir entrenamiento adicional/diferente (empleados, personal de IT, desarrolladores, lideres).
9) Identifique que va a comunicar a los diferentes grupos (el objetivo es el entrenamiento más corto posible que a la vez logre el mayor impacto).
10) *Identifique como va a comunicar el contenido-tres categorías de formación: nuevos, anuales, y en curso.*

B. Implementando el programa de concientización en seguridad

1) *Desarrolle y/o compre materiales de entrenamiento y contenido que cumpla con los requerimientos identificados durante la creación del programa.*
2) *Documente cuando y como planea medir el desempeño del programa.*
3) *Identifique a quien va a comunicar los resultados, cuando y como.*
4) *Despliegue el entrenamiento de concientización de seguridad utilizando diferentes métodos de comunicación identificados durante la creación del programa.*
5) *Implemente mecanismos de seguimiento para registrar quien y cuando completa el entrenamiento.*

C. Manteniendo el programa de concientización de seguridad

1) *Identifique cuando se revisara su programa de concientización de seguridad cada año.*
2) *Identifique amenazas cambiantes o nuevas o actualizaciones en los estándares que necesita incluir; incluya una actualización anual.*
3) *Desarrolle evaluaciones periódicas del conocimiento de seguridad de la organización y compare los resultados con la línea base.*
4) *Encueste al personal para obtener retroalimentación (utilidad, efectividad, facilidad de comprensión, facilidad de implementación, cambios recomendados, accesibilidad).*
5) *Mantenga el compromiso de la administración para soportar y promover el programa.*

D. Documente el programa de concientización de seguridad

1) *Documente el programa de concientización de seguridad incluyendo todo lo listado en los pasos anteriores "creando el programa de concientización sobre seguridad", "implementando el programa de concientización en seguridad" y "manteniendo el programa de concientización de seguridad".*

En las secciones a continuación encontraremos con más detalles algunos de los aspectos numerados en el anterior listado.

VII. METAS Y OBJETIVOS DEL PROGRAMA DE CONCIENTIZACIÓN

Como en la mayoría de los proyectos y procesos llevados a cabo dentro de una organización los programas de concientización deben establecer un conjunto de metas y objetivos, de lo contrario se arriesgarían a que como la mayoría de los procesos sin objetivos concluya en un fracaso.

El principal objetivo de definir una meta/objetivos es poder definir que deseo lograr con el proyecto/programa definiendo así mi foco y dirección.

Dentro del libro de McIlwraith encontramos algunos ejemplos de metas y objetivos que podrían tener nuestros programas así como algunos métodos para definirlos.

A. Formas de definición de los objetivos y metas

1) *Apoyarse en la pericia interna (algunas veces usando lo que se conoce como técnica Delphic).*
2) *Estadísticas internas actuales.*
3) *Involucrar a los interesados internos.*
4) *Evaluación de riesgos.*

B. Metas posibles de un programa de concientización

1) *Asegurarse de que todo el personal conozca cuáles son sus roles y responsabilidades frente a la seguridad de la información y actué conforme a ellos.*
2) *Ayudar a desarrollar y nutrir una cultura positiva frente a la seguridad en la organización que se enfoque en el esfuerzo de la seguridad de la información para incrementar los beneficios al reducir el riesgo.*

VIII. AUDIENCIA DE PROGRAMA DE CONCIENTIZACIÓN

Como en todo proceso de capacitación y entrenamiento la definición de la audiencia objetivo es importante para el correcto desarrollo de la actividad. Esta afirmación es aun más importante cuando estamos hablando de un proceso sobre un tema tan vital y segmentado dentro de las organizaciones como lo es el de la seguridad de la información. Cuando digo segmentado me refiero a que no todos los roles y cargos dentro de la organización tienen las mismas responsabilidades y por lo tanto también tendrían necesidades diferentes dentro del proceso de concientización.

La siguiente grafica (figura 1), extraída del documento *Best Practices for Implementing a Security Awareness Program* del PCI [11], nos muestra como se dividen las responsabilidades con respecto a la seguridad de la información de acuerdo al role dentro de una organización.

Figura 1. Responsabilidades vs Roles respecto a la seguridad de la información [11].

Por otra parte la grafica a continuación (ver figura 2), igualmente extraída del documento *Best Practices for Implementing a Security Awareness Program* del PCI [11], nos muestra de manera resumida como es la dependencia de los roles frente al contenido del programa de concientización, razón de más por la que es importante definir correctamente a la audiencia del programa.

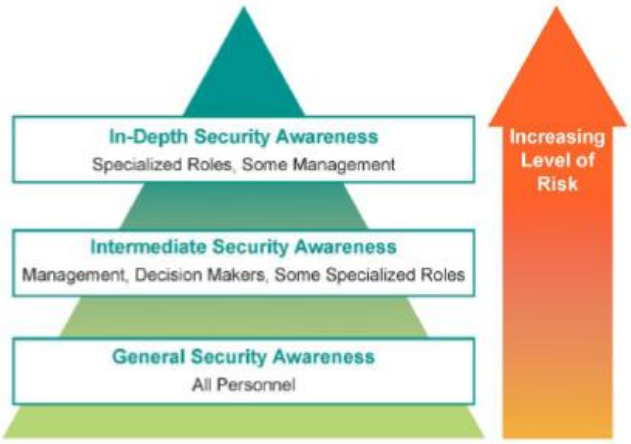

Figura 2. Necesidades de entrenamiento vs Roles [11].

Identificar la audiencia que va a ser parte del programa de concientización puede ser un proceso complicado en algunas organizaciones, especialmente las más grandes, sin embargo con la herramienta y metodología correcta esta tarea podría llevarse a cabo sin manera sencilla. Este es el caso del proceso que se realiza por medio de una matriz como lo aconseja el libro de McIlwraith. Según este autor al usar por ejemplo los siguientes factores dentro de una matriz se podría llegar a una clasificación efectiva y no compleja de la audiencia del programa:

1) *Escalón dentro de la organización (senior, intermedio, junior, etc).*
2) *Tipo de trabajo (profesional, administrativo, atención al cliente); personal de IT usualmente hacen parte de una audiencia especializada.*
3) *Localización física.*
4) *País.*
5) *Lenguaje.*
6) *Etnia.*
7) *Zona horaria.*

IX. TEMAS Y PUNTOS CON NECESIDADES DE CONCIENTIZACIÓN

Como vimos anteriormente es importante definir la audiencia de nuestro programa de concientización ya que estos tienen diferentes necesidades, pero como determinamos estas necesidades, como se logra determinar cuáles son las necesidades de entrenamiento que tiene el personal dentro de la organización.

De acuerdo al libro de McIlwraith, la evaluación de las necesidades de entrenamiento (TNA, training needs assessments) es el proceso que indica que temas y quienes necesitan entrenamiento. Dicha evaluación relacionara la población objetivo contra los conocimientos y habilidades requeridas. Usualmente para ejecutar correctamente la evaluación del requerimiento de entrenamiento se sigue la siguiente aproximación estructurada en pasos que se documentan en libro del autor:

A. Identificación del problema

Dentro de este punto se deben de identificar los incidentes presentes y recurrentes dentro de la organización, los riesgos y los cambios regulatorios o de estándares que apliquen.

B. Análisis

En este paso básicamente se realiza un análisis para encontrar la relación entre la causa de los problemas identificados en el punto anterior con respecto al conocimiento/habilidades del personal.

C. Identificación del las necesidades de entrenamiento

Finalmente, en este punto se determinan las habilidades/conocimientos que son necesarias por parte del personal para que se mitiguen los problemas anteriormente identificados.

Como punto importante dentro de la evaluación podemos considerar como se clasifica el conocimiento/habilidades de la población objetivo. Según este autor la clasificación se puede realizar de la siguiente manera:

1) *Cero conocimientos.*
2) *Conocimiento de bajo nivel de la terminología estándar.*
3) *Conocimiento de bajo nivel de alguna materia (normalmente adquirido informalmente).*
4) *Bajo nivel de entendimiento de alguna materia (incluido algo de teoría) normalmente adquirido mediante un método formal de aprendizaje; por ejemplo, el entrenamiento.*
5) *Alguna capacidad de aplicación práctica sobre la materia soportada por entrenamiento formal (quizás hasta un año de experiencia).*
6) *Alguna capacidad de aplicación práctica sobre la materia soportada por entrenamiento formal (de uno a dos años de experiencia).*
7) *Aplicación práctica prolongada soportada por una calificación formal de tipo académica o profesional (más de dos años de experiencia).*
8) *Reconocido experto en la industria con la habilidad de proveer consultoría y/o entrenamiento en la materia.*

X. SELECCIÓN DEL ENTRENADOR Y LOS MÉTODOS PARA EL PROGRAMA DE CONCIENTIZACIÓN

La correcta selección de los métodos y personas encargadas del proceso de concientización o entrenamiento

es otro aspecto fundamental que impacta directamente el éxito o fracaso del programa. Y al igual que con el punto anterior, en el que los temas dependían de la audiencia, la selección de estos dos aspectos también se ve influenciada por la audiencia objetivo del proceso de concientización.

En el caso de las personas encargadas de conducir el proceso, es necesario tener en cuenta que un buen entrenador debe combinar un correcto conocimiento en la materia con la habilidad de poder transmitir y enseñar el conocimiento que posee. Como usualmente no es posible encontrar a una persona que posea estos dos aspectos a un mismo nivel (alto por cierto), se debe de considerar la audiencia en su selección ya que usualmente cuando la audiencia posee un alto conocimiento en la materia, suele perder el interés e ir en contra del auditor si detecta falta de manejo de la materia en el. De manera análoga si la audiencia no posee conocimiento en la materia y el auditor no es capaz o posee la habilidad de transferir su conocimiento, estos terminaran adquiriendo poco o nada del conocimiento que se pretendía que adquieran.

Los métodos son afectados porque no todas las personas (las cuales poseen distintos niveles de escolaridad, edad, etnias, conocimiento) poseen las mismas capacidades de aprendizaje o facilidades de entendimiento según el método. Por ejemplo, nuevamente en el libro del autor McIlwraith, se nos indica que normalmente las audiencias conformadas por adultos suelen aprender o adquirir más conocimiento cuando los métodos de aprendizaje combinan diferentes medios/sentidos (sonido y vista por ejemplo).

Teniendo en cuenta esto, McIlwraith, lista los factores que normalmente influyen en la selección del método de entrenamiento. Estos factores son:

1) *Canales disponibles actualmente.*
2) *Geografía.*
3) *Objetivos del programa.*
4) *Localización de la audiencia y distribución.*
5) *Ventanas de disponibilidad de tiempo.*

El quinto punto de la anterior lista tiene especial importancia con un tema que puede llegar a ser muy técnico y extenuante, como lo es la seguridad de la información, si por ejemplo se dictan largas horas de cátedra de manera consecutiva.

Teniendo en cuenta los factores listados por el autor, se debe realizar la selección de los métodos de entrenamiento del programa para los cuales se pueden considerar por ejemplo los seminarios, métodos multimedia (los conocidos webinars), conferencias o incluso los entrenamientos basados en aplicaciones de computador (CBT, computer bases training).

XI. ACTUALIZACIÓN Y EVALUACIÓN DEL PROGRAMA DE CONCIENTIZACIÓN

Como en la mayoría de las demás aéreas de la tecnología, la seguridad de la información es una materia en constante evolución y cambio; por lo tanto, todo programa exitoso de concientización sobre la seguridad de la información debe de tener un componente de evaluación y actualización del programa que garantice que este sea vigente y adecuado para el contexto en el que se mueve la organización.

Adicionalmente cabe recordar que no solamente la materia de la seguridad de la información es la que evoluciona constantemente, cambios internos dentro de la organización y cambios en el mercado y la competencia pueden motivar y provocar una evolución en los procesos y finalmente la necesidad de modificar los programas de concientización para adaptarse a las nuevas necesidades de la organización.

Para este capítulo, cambiando de libro y autor, voy a tomar las recomendaciones de la *Computer Security Division* [13] del NIST para realizar el proceso de evaluación y retroalimentación del programa de concientización. En la siguiente grafica (ver figura 3) se resumen los diferentes mecanismos que pueden ser usados para la evaluación y retroalimentación según el NIST.

Figura 3. Mecanismos de evaluación y retroalimentación [13].

A continuación incluyo lo indicado por el NIST para cuatro de estos mecanismos:

1) *Formularios de evaluación/Cuestionarios: Pueden ser usados varios formatos. Los mejores diseños eliminan la necesidad de que las personas que los completan escriban mucho. La clave es diseñar el formulario para que sea amigable con el usuario. Trabaje con expertos internos que estén familiarizados con las mejores técnicas de diseño para estos instrumentos o busque asistencia de expertos externos.*
2) *Grupos focales: Traiga temas del entrenamiento a los foros abiertos para discutir sus puntos de vistas acerca de la efectividad del entrenamiento*

en seguridad de la información y solicitar ideas para su mejoramiento.

3) *Entrevistas selectivas: Para esta propuesta lo primero que se realiza es la identificación de grupos de entrenamiento objetivos basados en el impacto, prioridad u otros criterios establecidos e identificar las aéreas específicas para la retroalimentación. Normalmente se realizan usando entrevistas uno a uno o en pequeños grupos homogéneos (usualmente diez o menos), este enfoque es más personalizado y privado que el enfoque de grupos focales y puede motivar a los participantes a estar más dispuesto a ser críticos con el programa.*
4) *Análisis u observación independientes: Otra propuesta para solicitar retroalimentación es la incorporación de la revisión del programa de concientización en seguridad informática como una tarea de un contratista externo o de cualquier tercero como parte de una auditoria. La organización podrá hacer esto adicionalmente a las actividades de supervisión para obtener una opinión imparcial de la efectividad del programa.*

XII. CONCLUSIONES

Las personas son un factor importante dentro del contexto de la seguridad de la información y juegan un papel determinante en el correcto o incorrecto desempeño (desde el punto de vista de la seguridad) de los sistemas de información. Pero para que estas personas se conviertan en factores que potencialicen la seguridad de los sistemas de información deben recibir el correcto apoyo por parte de los profesionales de la seguridad de la información, los equipos de desarrollo y los analistas que desarrollan los controles, sistemas e interfaces de usuario. Dicho apoyo podría resumirse dentro de las siguientes tres categorías principales:

- Concientización acerca de la seguridad de la información y la importancia de cada persona para alcanzar los objetivos de seguridad.
- Diseño amigable y simple de las interfaces que facilite su uso por parte del usuario.
- Diseño de los proceso, o al menos de los puntos en donde intervienen las personas, teniendo en cuenta los modelos mentales y capacidades cognitivas de las personas de tal manera que faciliten las decisiones y minimicen el desgaste de la persona durante el uso del sistema.

REFERENCIAS

[1] M. Rouse. (2005, Sep) What is HCI (human-computer interaction)? [Online].Available:http://searchsoftwarequality.techtarget.com/definition/HCI-human-computer-interaction

[2] F. J. Haeussinger, J. J. Kranz. (2013, Dec). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. Presented at International Conference on Information Systems 2013. [Online]. Available: https://www.uni-goettingen.de/de/document/download/7b9bef1bc07f19dd87d65e95783d8c20.pdf/Information_Security_Awareness-Haeussinger_Kranz_%202013.pdf

[3] Brad A. Myers. "A Brief History of Human Computer Interaction Technology." ACM interactions. Vol. 5, no. 2, March, 1998. pp. 44-54.

[4] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," MIS Quarterly, (34:3), pp. 523-A527.

[5] Ka-Ping Yee. "User Interaction Design for Secure Systems" University of California, Berkeley, CA, UCB/CSD-02-1184, 2002.

[6] U. Jendricke and D. Gerd tom Markotten. Usability meets Security: The Identity-Manager as your Personal Security Assistant for the Internet. In Proceedings of the 16th Annual Computer Security Applications Conference, December 2000.

[7] A. Adams and M.A. Sasse, "Users are Not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures," Comm. ACM, vol. 42, no. 12, 1999, pp. 41–46

[8] S.W. Smith. (2003, May.). Humans in the Loop: Human–Computer Interaction and Security. *IEEE Security & Privacy Magazine*.[online]. Available: http://www.cs.dartmouth.edu/~sws/pubs/humans.pdf

[9] L. Zinatullin, "The Psychology of Information Security-Resolving conflicts between security compliance and human behavior" 1st ed, IT Governance Publishing, UK, 2016.

[10] G. Kosaka. Shell. (2008, May) NSI.org. [Online]. Available: https://www.nsi.org/pdf/awarness-articles/5%20Ways%20to%20Employee%20Awareness.pdf

[11] Security Awareness Program Special Interest Group PCI Security Standards Council. (2014, Oct). NSI.org. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

[12] McIlwraith, A. (2006, Aug). Information Security and Employee Behavior: How to Reduce Risk Through Employee Education, Training and Awareness. Abingdon, GB: Gower. Retrievedfromhttp://www.ebrary.com

[13] M. Wilson, J. Hash. (2003, Oct) Building an Information Technology Security Awareness and Training Program. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[14] Desman, M. B. (2001, Oct). Building an Information Security Awareness Program. London, GB: Auerbach Publications. Retrieved from http://www.ebrary.com

Autor

Jorge Andrés Rojas Valencia. Ingeniero informático. Actualmente se desempeña tareas de pruebas de software para clientes locales e internacionales para la empresa Globant.