Guía para la Elaboración de un Plan de Concientización y Entrenamiento, sobre Seguridad de la Información

Diego Mauricio Álvarez Bernate.
diego.alvarez.bernate@gmail.com;
Especialización en Seguridad Informática
Universidad Piloto de Colombia – Bogotá, Colombia.

***Resumen*— Las empresas al tratar temas sobre seguridad de la información piensan solo en hardware y en la preocupación de invertir grandes cantidades de dinero y esfuerzos en tecnología, pero han dejado a un lado a las personas a sus funcionarios y colaboradores y sin saberlo han hecho que ellos sean el eslabón más débil de la cadena en temas de seguridad dentro de la organización.**

Por lo anterior se hace necesario dentro de las organizaciones el desarrollar un plan de concientización y entrenamiento sobre seguridad de la información para sus funcionarios, permitiendo mitigar el riesgo al que está expuesta la organización y el cual describiremos como guía en este documento.

***Abstract*— The companies when dealing with issues of information security think only about hardware and the concern to invest large amounts of money and efforts in technology, but have left people aside their employees and employees and unknowingly have made they are the weakest link in the chain in security issues within the organization.**

Therefore it is necessary within the organizations to develop a plan of awareness and training on information security for its officials, allowing to mitigate the risk to which the organization is exposed and which we will describe as a guide in this document.

Índice de Términos: **Concientización, Entrenamiento Seguridad de la información, Usuarios**.

I. INTRODUCCIÓN

En los últimos años los sistemas de información, se han convertido en una parte importante para las organizaciones permitiéndoles optimizar los procesos internos haciendo que las empresas sean más eficientes cada día.

A su vez este uso de la tecnología ha permitido el surgimiento de nuevas amenas y vulnerabilidades, que pueden llegar a afectar la disponibilidad, confidencialidad e integridad de la información pilares de la seguridad de la información que cualquier empresa sin importar su razón de ser debe proteger y garantizar con el fin de no ver afectado el desempeño normal de la organización.

La mayoría de las organizaciones asumen la seguridad de la información de manera que solo es responsabilidad del área de tecnología y que esta se subsana con la compra de dispositivos y/o software específicos como por ejemplo antivirus, antimalware, pero no se dan cuenta que sin importar que tanta sea la inversión que se halla hecho en tecnología siempre estarán expuesto, si no ven a sus funcionarios como una parte importante de la seguridad de la información.

Por lo tanto es importante invertir en capacitarlos sobre los riesgos a los que esta expuestos tanto ellos como las organizaciones en una mundo donde la tecnología y las redes de comunicaciones están aún solo clics de distancia.

La finalidad de este documento es ser una guía en la elaboración del Plan de Concientización y Entrenamiento sobre Seguridad de la Información en base a la NIST SP 800-50 y las ISO/IEC 27001:2013, 27002:2013.

II. DESCRIPCIÓN GENERAL

Un plan efectivo de concientización y entrenamiento en seguridad de la información debe explicar de la manera más apropiada las reglas de comportamiento para el uso de los sistemas de informáticos, las cuales deben estar plasmadas generalmente en las políticas y procedimiento de seguridad de la información de la organización que requiere que sean cumplidos y acatados por parte de todos los usuarios del sistema.

Teniendo en cuenta lo anterior, en la elaboración de un plan de concientización y entrenamiento sobre seguridad de la información, la NIST Special Publication SP-800-50 “Construcción de un Programa de Concientización y Entrenamiento de Seguridad de Tecnologías de Información”, nos proporciona una guía para la elaboración de dicho programa.

Dicho documento establece de manera clara la diferencia entre los tres componentes principales de un programa para desarrollar la cultura en seguridad de la información: concientización, entrenamiento y educación:

- Concientización: Su propósito es enfocar la atención en seguridad de la información para posibilitar que el público objetivo reconozca los temas de interés, estableciendo al inicio qué comportamientos se quieren reforzar, por ejemplo,

mantener el escritorio limpio, usar de forma adecuada las contraseñas, elaborar copias de respaldo, usar el correo responsablemente, etcétera.

- Entrenamiento: Se centra en producir habilidades y competencias en seguridad de la información relevantes y requeridas con el fin de que el público objetivo las aprenda y aplique en el día a día.
- Educación: Integra habilidades de seguridad y competencias de las diferentes especialidades funcionales dentro de un cuerpo común de conocimientos, enfocándose en producir especialistas en seguridad.

En este ciclo el aprendizaje es continuo, ya que inicia con concientización y prosigue con el entrenamiento y desarrollo a través de la educación hacia la creación de cultura de seguridad de la información. (Carlos Villamizar R. CISA, 2013)

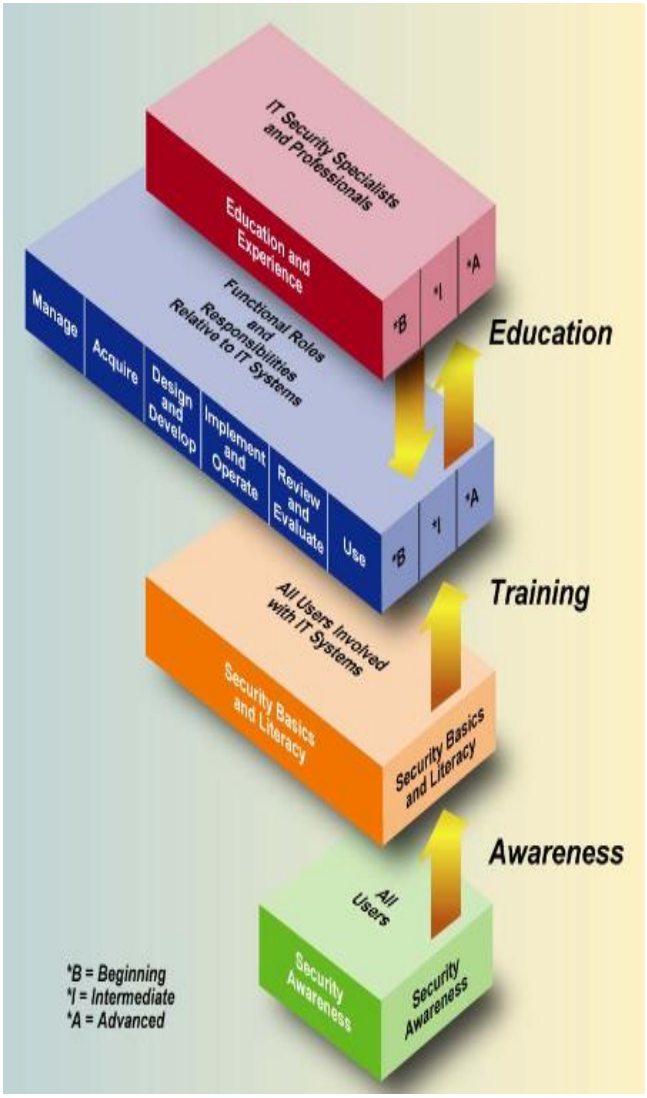

Fig. 1. El continuo de aprendizaje de seguridad de TI [1]

La NIST SP 800-50 identifica cuatro pasos críticos en el ciclo de vida de un programa de concientización y entrenamiento de seguridad de la información:

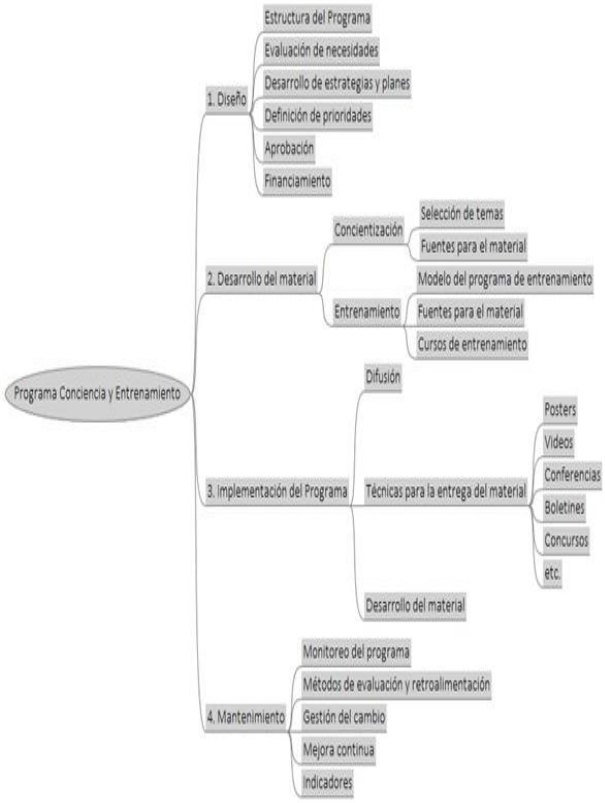

Fig. 2. Fases ciclo de vida de un programa de concientización y capacitación en seguridad de TI [2]

A. Diseño del plan de concientización y entrenamiento.

En este paso, el área de seguridad de TI necesita evaluar la estrategia de entrenamiento que será desarrollada y aprobada, es importante que el programa de concientización y entrenamiento apoye las necesidades de negocio y sea relevante a la cultura organizacional.

El diseño del plan de concientización y entrenamiento, se encuentra compuesto de los siguientes puntos:

1) Estructuración de un área de concientización y entrenamiento

- Modelo 1: Programa Centralizado- En este modelo, la responsabilidad y el presupuesto para toda el área de TI en materia de concientización y programas de capacitación se otorgan en una autoridad central.
- Modelo 2: Programa Parcialmente Descentralizada - En este modelo, la seguridad de la concientización y entrenamiento se definen por una autoridad central, pero la ejecución se delega a la línea de gestión de los funcionarios de la organización. La asignación de presupuesto, el desarrollo del material y la programación para

el área de concientización y entrenamiento son responsabilidad de estos funcionarios.

- Modelo 3: Totalmente Descentralizado - En este modelo, la autoridad central del área de seguridad de concientización y entrenamiento difunde las expectativas generales de políticas de concientización en materia de seguridad y requisitos de entrenamiento, pero otorga la responsabilidad de la ejecución del programa en su totalidad a otras dependencias.

2) Evaluación de necesidades

La evaluación de las necesidades es un proceso que puede ser empleado para determinar las necesidades de concientización y entrenamiento dentro de la organización. Los resultados de la evaluación pueden proporcionar la justificación necesaria para que la alta gerencia de las organizaciones proporcione los recursos necesarios para satisfacer las necesidades detectadas.

Algunos de estos métodos con los que podemos medir el estado actual de la organización son:

- Entrevistas con grupos o usuarios claves dentro de la organización
- Encuestas organizacionales.
- Verificar comportamientos generales del personal (sesiones abiertas, escritorios limpios)
- Verificación de los incidentes de seguridad de la información
- Análisis de los eventos registrados en los dispositivos de seguridad (firewall, IDS/IPS, SIEM) o intrusiones en páginas web, con que cuente la organización.

3) Desarrollo de las estrategias y planes de concientización y entrenamiento

Después de terminar con la evaluación de las necesidades, obtendremos la información necesaria para iniciar con la estrategia de desarrollo, implementación y mantenimiento del plan de concientización y entrenamiento.

Una vez se hayan identificado todas las falencias dentro de la organización, se debe proceder con la elaboración del plan, el cuál debe contener entre otros los siguientes elementos:

- Alcance del plan.
- Objetivos del plan
- Roles y responsabilidades.
- A quien va dirigido
- Temas a ver en cada sesión.
- Frecuencia de las capacitaciones
- Evaluación y renovación del material creado.

4) Establecimiento de prioridades

La finalidad, es desarrollar un calendario de aplicación, sobre todo si existen limitaciones presupuestarias y disponibilidad de recursos, este calendario permitirá determinar la secuencia y prioridad para cuando se tengan que definir prioridades.

5) Elección del material en función del personal.

Este apartado manifiesta que es necesario tomar una decisión en cuanto a la complejidad del material que será desarrollado en función del personal. La complejidad debe ser acorde con la función de la persona que vaya a someterse al esfuerzo del aprendizaje.

La complejidad del material, debe ser determinada antes del desarrollo, esta decisión aplica a los tres tipos de aprendizaje (concientización, entrenamiento y educación)

Esto se debe a que no es lo mismo realizar un material de entrenamiento aun grupo específico de usuario donde buscamos que el usuario después de ser entrenado adquiera unas habilidades específicas para sus labores, a un material de sensibilización donde buscamos disuadir a los usuarios a comportarse de determinada manera, para evitar consecuencias tanto para él, como para la organización.

6) Financiamiento del programa de seguridad de concientización y entrenamiento

Después de definir la estructura del plan y su complejidad se debe realizar el estimado de recursos financieros necesario para el desarrollo del plan.

La idea es enviar un mensaje claro a la alta dirección de que de ahora en adelante debe existir un presupuesto definido para desarrollar los planes de capacitación

B. Desarrollo del material de concientización y entrenamiento

Este paso se enfoca en fuentes de educación disponibles, alcance, contenido y desarrollo del material para el entrenamiento.

El desarrollo del material de concientización y entrenamiento, debe garantizar el comportamiento que se quiere reforzar y por otro lado, las habilidades o destrezas que se quiere que la audiencia aprenda y aplique.

Mientras que el mensaje en el material de entrenamiento debe garantizar que incluirá todo lo necesario para que los participantes puedan realizar su trabajo de manera satisfactoria, el material de concientización busca hacer del conocimiento de la audiencia, las implicaciones legales y responsabilidades en materia de seguridad informática a las que se hacen acreedores, mientras se encuentran laborando en la organización.

La idea fundamental del desarrollo de este material es que los empleados entiendan que la seguridad de la información es una responsabilidad compartida y que todos son importantes en esa labor.

1) Desarrollo de material de concientización.

Una de las cuestiones que se plantea cuando se comienza a desarrollar el material para el plan de concientización y entrenamiento en una organización es ¿Qué requiere conocer

el personal de la organización en materia de seguridad de la información?

La cantidad de temas que pueden incluirse en el plan de concientización y entrenamiento, puede ser muy extensa, la siguiente es una lista de los temas que pueden incluirse como parte de este plan: [3]

- Uso y administración de contraseñas: incluida la creación, la frecuencia de los cambios y la protección.
- Protección contra virus, gusanos, caballos de Troya y otros códigos maliciosos: escaneo, actualización de definiciones.
- Política: implicaciones de incumplimiento.
- Correo electrónico / archivos adjuntos desconocidos.
- Uso de la web: permitido vs prohibido; monitoreo de la actividad del usuario.
- Spam.
- Copia de seguridad y almacenamiento de datos: enfoque centralizado o descentralizado.
- Ingeniería social.
- Respuesta al incidente - ¿contactar a quién? ¿Qué debo hacer?
- Mirar por encima del hombro.
- Cambios en el entorno del sistema: aumentan los riesgos para los sistemas y los datos (por ejemplo, agua, fuego, polvo o tierra, acceso físico).
- Inventario y transferencia de propiedad: identifique la organización responsable y las responsabilidades del usuario.
- Problemas de uso y ganancia personal: sistemas en el trabajo y en el hogar.
- Problemas de seguridad de dispositivos de mano: abordan problemas de seguridad física e inalámbrica.
- Uso del cifrado y la transmisión de información delicada / confidencial a través de Internet: dirija la política de la agencia, los procedimientos y el contacto técnico para obtener asistencia.
- Seguridad de la computadora portátil mientras viaja: aborde los problemas físicos y de seguridad de la información.
- Sistemas y software de propiedad personal en el trabajo: establezca si está permitido o no (por ejemplo, derechos de autor).
- Aplicación oportuna de parches del sistema: parte de la gestión de la configuración.
- Problemas de restricción de licencia de software: dirección cuando las copias están permitidas y no permitidas.
- Software admitido / permitido en sistemas de organización: parte de la gestión de configuración.
- Problemas de control de acceso: menos privilegios y separación de tareas.
- Uso de declaraciones de acuse de recibo: contraseñas, acceso a sistemas y datos, uso personal y ganancia.
- Control de visitantes y acceso físico a los espacios: discute la política de seguridad física y los procedimientos aplicables, por ejemplo, desafía a extraños, informa actividad inusual.
- Seguridad en el escritorio: discuta el uso de protectores de pantalla, restringiendo la visualización de la información en la pantalla por parte de los visitantes, dispositivos de respaldo de batería, acceso permitido a los sistemas.
- Proteja la información sujeta a preocupaciones de confidencialidad: en sistemas, archivados, en medios de respaldo, en forma impresa y hasta que se destruya.
- Etiqueta de la lista de correo electrónico: archivos adjuntos y otras reglas.

2) Desarrollo de material de entrenamiento

Como se vio en la introducción de este apartado, uno de los planteamientos cuando se inicia el desarrollo del material para programa de entrenamiento específico es ¿Qué habilidades o destrezas se necesitan hacer llegar a la audiencia? Al respecto el NIST SP 800-16 “Requerimientos para entrenamiento en Seguridad de Tecnologías de la Información: Modelo basado en rendimiento y roles”, plantea un metodología para la creación de cursos de formación para una serie de audiencias.

Podemos obtener diverso materia para el desarrollo del plan de diferentes fuentes como son:

- Organizaciones profesionales y proveedores de seguridad de la información.
- Periódicos.
- Conferencias de seguridad
- Seminarios online
- boletines sobre seguridad en sitios web.

C. Implementación del Plan

Este paso direcciona la comunicación eficaz y los roles del plan de concientización y entrenamiento.

Como primera medida se debe socializar con la alta gerencia de la organización, esto nos garantizara el apoyo y los recursos necesarios para su ejecución y así dar inicio a la implementación

A continuación se describe algunas técnicas que permiten difundir o comunicar la información, la selección de cada método debe ser acorde a los recursos y tecnología con que cuenta la organización, algunos ejemplos son: [4]

- Posters con mensajes o checklist sobre que debe y que no debe hacerse.
- Videos institucionales a través de videowalls o pantallas.
- Screensavers con mensajes de sensibilización.

- Cuadernos, relojes o elementos de oficina con mensajes alusivos.
- Boletines vía email.
- Eventos relacionados con seguridad, concursos etc.
- Sesiones con instructores (si se planean charlas que contengan varios temas de sensibilización a la vez).

De acuerdo al NIST en la publicación SP800-50, la implementación de un programa de concientización y entrenamiento debería aplicarse sólo después de que:

- Se ha llevado a cabo una evaluación de necesidades.
- Se ha desarrollado una estrategia.
- Se ha completado un programa de concientización y entrenamiento.
- Se ha desarrollado el material de concientización y entrenamiento.

D. Mantenimiento del Plan

Este paso de la guía se orienta al cuidado y monitoreo del plan. Los métodos de retroalimentación eficaces pueden incluir revisiones, grupos de interés, pruebas de referencia, por citar algunos.

Es necesario asegurar que el plan, como estructura, sigue siendo actual aún con la nueva tecnología y las cuestiones de seguridad que aparezcan. Se deberá centrar en las necesidades de formación con nuevas habilidades y capacidades de ser necesario, para responder a los nuevos cambios tecnológicos.

Un plan de concientización y entrenamiento, no podrá mejorarse, sin antes saber cómo se está desempeñando al interior de la organización, para ello, es necesario buscar métodos que nos indiquen la efectividad del programa.

Dentro de los métodos más comunes para evaluar las campañas de concientización y entrenamiento son:

- Evaluaciones o cuestionarios.
- Foros Abiertos con usuarios que recibieron la capacitación.
- Entrevistas selectivas o entrevistas grupales.
- Uso de observadores independientes o auditores, que evalúen la efectividad del programa.
- Uso de "benchmarking", que indica comparar el método que se ha implementado con el de otras empresas similares, para así mejorar el modelo implementado.
- Verificación de la cantidad de incidentes abiertos y su causa
- Ataques de ingeniería social, posteriores a las capacitaciones.

Fig. 3. Técnicas de evaluación y retroalimentación [5]

Los resultados obtenidos en esta fase del plan deben ser comparados con los resultados obtenidos de la fase de diseño, lo que nos permite obtener un indicador de desempeño, el cual será nuestro punto de partida para determinar que se debe mejorar en el plan de capacitaciones.

Es necesario que siempre exista un mejoramiento por más mínimo que sea, ya que se corra el riesgo de que el plan se vuelva obsoleto y luego se requiera de mucho más esfuerzo para ponerlo a punto nuevamente.

III. GLOSARIO DE TÉRMINOS

- *Activos de información*. Recurso de valor para el desarrollo de la actividad propia de la Institución que incluye la gestión de la información, el software para su tratamiento y los soportes físicos y lógicos de la información.
- *Amenaza.* Cualquier elemento o acción que es capaz de aprovechar una vulnerabilidad y comprometer la seguridad de un sistema de información.
- *Confidencialidad.* Uno de los tres principios básicos (los otros dos son el principio de integridad y el de disponibilidad) de la implementación de la seguridad de la información. La confidencialidad implica que debe protegerse la información de forma tal que sólo sea conocida por las personas autorizadas y se la resguarde del acceso de terceros.
- *Disponibilidad.* Uno de los tres principios básicos (los otros dos son el principio de integridad y el de confidencialidad) de la implementación de la seguridad de la información. La disponibilidad implica que debe protegerse la información de forma tal que se pueda disponer de ella para su gestión en el tiempo y la forma requeridos por el usuario.
- *Hardware.* Término en inglés que hace referencia a cualquier componente físico tecnológico, que interactúa de algún modo con

un sistema computacional.

- *ISO.* International Organization for Standardization. Entidad internacional encargada de favorecer la estandarización en el mundo.
- *Incidente*. El equipo de Coordinación de Emergencias en Redes Teleinformáticas (ArCERT) define este término como un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de quebrar los mecanismos de seguridad existentes. Una violación o inminente amenaza de violación de una política de seguridad de la información o política de uso aceptable de recursos de información.
- *Información.* Conjunto de datos que toman sentido al integrarse con características comunes.
- *Informática.* La informática es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora.
- *Ingeniería Social*. Es un método basado en el engaño y la persuasión que puede llevarse a cabo a través de canales tecnológicos o bien en persona, y que se utiliza para obtener información significativa o lograr que la víctima realice un determinado acto. Un ejemplo de la aplicación de esta técnica es el phishing.
- *Integridad.* Uno de los tres principios básicos (los otros dos son el principio de confidencialidad y el de disponibilidad) de la implementación de la seguridad de la información. La integridad implica que debe salvaguardarse la totalidad y la exactitud de la información que se gestiona.
- *Malware (software malicioso),* Software diseñado para ejecutar acciones maliciosas (como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario) y que incluye programas como virus, gusanos, troyanos y spyware. Puede utilizar como vía de diseminación, el correo electrónico, sitios de internet, redes, dispositivos móviles, dispositivos removibles (por ejemplo pen-drives).
- *Pishing. (Del inglés fishing: pesca).* Fraude informático efectuado a través de una comunicación electrónica. Es un proceso fraudulento de la rama de la social cuyo objetivo es adquirir información sensible, como nombres de usuarios, contraseñas y números de tarjetas de crédito.
- *Políticas.* Actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. Acción elegida como guía en el proceso de toma de decisiones al poner en práctica o ejecutar las estrategias, programas y proyectos específicos del nivel institucional.
- *Red.* Es una serie de computadores o dispositivos que se encuentran conectados entre sí, por un medio físico (cable) o de manera inalámbrica donde se comparte información, recursos y los servicios.
- *Riesgo.* Es la posibilidad de que una amenaza aproveche una vulnerabilidad y dañe un activo de información.
- *SGSI*. Sistema de gestión de la seguridad de la información.
- *Seguridad de la información*. Conjunto de metodologías, técnicas, estrategias, políticas, normas y procedimientos tendientes a minimizar las amenazas y riesgos continuos a los que está expuesta la información, con el fin de asegurar la continuidad de las operaciones de la Institución cumpliendo con la preservación de los tres principios básicos: integridad, confidencialidad y disponibilidad de la información.
- *Seguridad* Informática. Conjunto de metodologías, políticas, técnicas, estrategias y procedimientos orientados a proteger un sistema informático procurando preservar la integridad, disponibilidad y confidencialidad de la información procesada en un sistema de computadoras.
- *Vulnerabilidad.* Debilidad en un activo que lo hace susceptible de ser atacado.

IV. CONCLUSIONES

La información en los últimos años se ha vuelto en el activo más importante y de mayor valor para las organizaciones, la cual se debe proteger a todo momento de posibles ataques o de fugas de información, por tal motivo el área de tecnología garantizar la integridad, confidencialidad y disponibilidad de la información.

El usuario final es clave para el desarrollo de un programa de gestión de la seguridad de la información, sin un usuario sensibilizado acerca de las amenazas y vulnerabilidades a los que está expuesto, es más probable que se produzcan incidentes de seguridad que puedan a tener impacto considerable dentro de la organización.

El apoyo y compromiso de la alta dirección es clave para poder llevar a cabo un buen plan de capacitación.

Las métricas son fundamentales para el mejoramiento continuo de cualquier proceso de gestión de seguridad incluyendo el de capacitación y sensibilización.

REFERENCIAS

[1] NIST Special Publication 800-50, Pág. 8
[2] HYPERLINKhttp://www.magazcitum.com.mx/?p=2361#.W7Jf22hKjDc Posts by Carlos Villamizar R. CISA, CISM, CGEIT, CRISC, CobiT Foundation Certificate e ISO27001 LA". Jugando a crear cultura de seguridad de la información – De la teoría a la práctica (Agosto 2013).
[3] NIST Special Publication 800-50, Pág. 24
[4] NIST Special Publication 800-50, Pág. 33
[5] NIST Special Publication 800-50, Pág. 37

BIBLIOGRAFÍA

[1] 27001Academy. (s.f.). Advisera.com. Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/
[2] NIST (National Institute Of Standards And Technology) Special Publication 800-50 Building an Information Technology Security Awareness and Training Program.
[3] ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident management
[4] Departamento de seguridad informática, Universidad Nacional de Luján. http://www.seguridadinformatica.unlu.edu.ar/?q=lexicon/1
[5] ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary
[6] ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements