Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 14

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSION	FECHA	CAMBIOS INTRODUCIDOS
1.0	17/03/2016	Versión Inicial Del Documento

TABLA DE CONTENIDO

PÁG.

INDICE DE TABLAS

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27000 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

2. AUDIENCIA

Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

En la última década, las tecnologías de información y comunicaciones se han convertido en la herramienta por excelencia para la optimización de los procesos y el funcionamiento eficaz de una empresa.

Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la disponibilidad, privacidad e integridad de la información que se encuentra disponible en las diferentes plataformas, afectando de esta manera el desempeño normal de la Entidad.

Para esto, el modelo de seguridad y privacidad indica pautas específicas para guiar a las instituciones a robustecer sus plataformas y mitigar amenazas que pueden llegar a traer consigo las tecnologías implementadas, sin embargo, un programa robusto de seguridad y privacidad de la información no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar los factores humanos, que en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido a que no conocen sobre seguridad de la información y su rol dentro de una Entidad.

Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información.

4. OBJETIVOS

Este documento tiene como objetivo establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, cubra en su totalidad los funcionarios de la Entidad, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de las entidades del Estado, se busca:

- Definir los temas para la capacitación en seguridad de la información, de acuerdo con el público objetivo.
- Establecer la metodología que les permita evidencias cuales son las necesidades de capacitación para la entidad.
- Construir materiales para sensibilización y entrenamiento.
- Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades de la Entidad.

5. GLOSARIO

- **Sensibilización**: Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

- **Entrenamiento**: Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

- **Política**: Declaraciones de alto nivel que expresan los objetivos a cumplir de la Entidad respecto a algún tema en particular.

- **Brecha**: Se denomina al espacio o ruta a recorrer entre un estado actual y un estado deseado.

- **Ingeniería Social**: "Tipo de ataque de seguridad en la cual un individuo manipula al otro con el fin de obtener información que puede ser utilizada para acceder a un sistema no autorizado, sustraer dinero o incluso suplantar la identidad de la víctima"[1].

[1] Complete Guide To CISM Certification, Pág. 191.

6. DESCRIPCIÓN GENERAL DEL PLAN DE SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN

Un programa efectivo de sensibilización, capacitación y comunicación en seguridad de la información debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema.

Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad.

Teniendo en cuenta lo anterior, un plan de capacitación, sensibilización y comunicación adecuado, debe llevarse a cabo con base a las siguientes 4 fases:

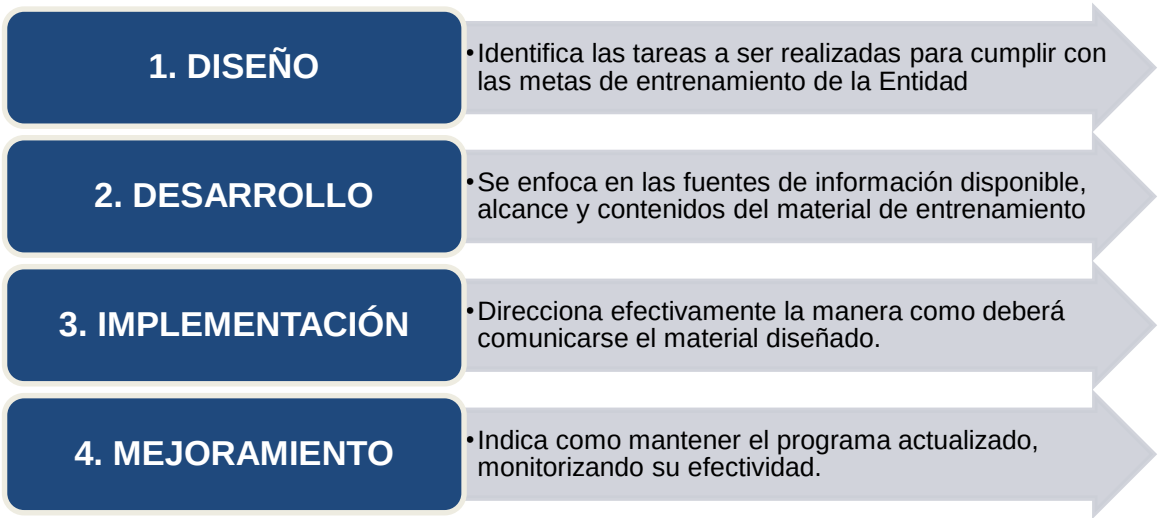

Figura 1. Fases plan de sensibilización, capacitación y comunicación

7. DIFERENCIAS ENTRE SENSIBILIZACIÓN, ENTRENAMIENTO, EDUCACIÓN Y DESARROLLO PROFESIONAL

Previo a la identificación de cada una de las fases, es conveniente definir y diferenciar los siguientes términos: SENSIBILIZACIÓN, ENTRENAMIENTO, EDUCACIÓN y DESARROLLO PROFESIONAL ya que cada uno de ellos tiene un fin particular dentro del plan y dentro de la Entidad.

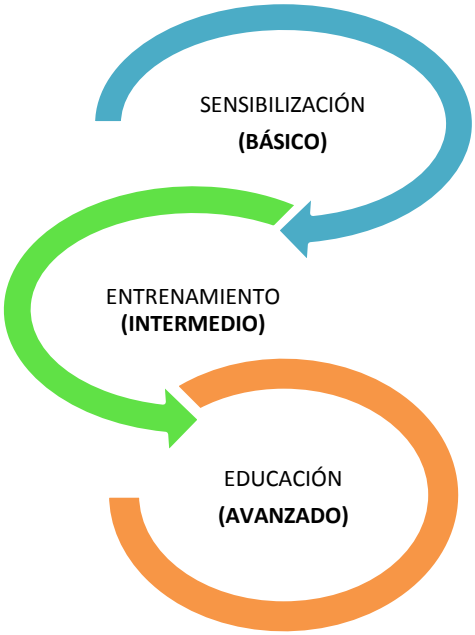

Figura 2. Relación Entre Sensibilización, Capacitación Y Educación

7.1. SENSIBILIZACIÓN:

Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

EJEMPLO: Uso correcto de contraseñas, consecuencias reales sobre prestar una contraseña y qué hacer si no recuerdo mi contraseña.

El éxito de la sensibilización es la practicidad y la simplicidad en que esta información es entregada, para captar la atención del aprendiz.

7.2. ENTRENAMIENTO:

Busca enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo. Un programa de entrenamiento no busca certificar (aunque puede llegar a hacerlo), pero puede tener mucha temática relacionada con un curso de certificación.

EJEMPLO: Un curso de seguridad de la información, enfocado a administración de riesgos, ciclo de vida del servicio de seguridad y controles operacionales. Un curso sobre administración de plataformas de verificación de registros (Log).

7.3. EDUCACIÓN FORMAL:

Se define como todos los niveles y habilidades de seguridad envueltos en un único cuerpo de conocimiento.

EJEMPLO: Programa de estudios de educación superior, postgrados, etc…

7.4. DESARROLLO PROFESIONAL (EDUCACIÓN NO FORMAL):

Busca asegurar que los usuarios desde el más principiante hasta el más experimentado, tengan los conocimientos suficientes para desempeñar sus roles. Esto se logra a través de certificaciones, que ofrecen proveedores de plataformas específicas, sistemas operativos etc… o algunas otras relacionadas con conceptos de seguridad informática (gestión, planeación etc…).

Esta parte de desarrollo profesional, depende de cada institución si requiere de certificaciones para desempeñar bien sus roles o si son motivo para brindar algún tipo de bonificación adicional al empleado por su preparación.

8. DISEÑO DEL PROGRAMA DE SENSIBILIZACIÓN Y CAPACITACIÓN

El programa debe ser diseñado teniendo presente la misión de la Entidad y la relevancia que se busca para la cultura de la Entidad.

En este paso deben ser identificadas las necesidades y las prioridades que tenga la compañía respecto al tema de entrenamiento y sensibilización de su personal, para procurar un buen diseño del programa.

En esta fase debe estructurar el programa, establecer los niveles de complejidad y como financiar dicho programa.

El primer paso, será seleccionar el modelo como se administrará el programa de sensibilización.

8. MODELOS DE ADMINISTRACIÓN DE UN PROGRAMA DE ENTRENAMIENTO Y SENSIBILIZACIÓN:

Existen 3 modelos base que permiten administrar un programa de entrenamiento y sensibilización:

Modelo 1. Política, Estrategia e Implementación Centralizadas (Modelo Centralizado).
Modelo 2. Política y Estrategia Centralizada, Implementación Distribuida (Parcialmente Descentralizado).

El uso de cada modelo dependerá del tamaño de la Entidad, número de empleados, sedes y presupuesto disponible.

8.1. MODELO 1. CENTRALIZADO:

En este modelo, todo corre por cuenta del ente principal de la compañía, es decir, las políticas, la estrategia y la implementación, son fijadas por el ente principal y luego distribuido de igual manera a todas sus sedes (unidades organizacionales) para que sea aplicada de manera homogénea en cada una.

Este modelo se recomienda para entidades con una única sede, aunque si la entidad considera que tiene la experticia y control suficiente para dirigir todas sus sedes desde su ente principal, es una opción viable.

8.2. MODELO 2. PARCIALMENTE DESCENTRALIZADO:

En este modelo, las políticas y la estrategia son definidas por el ente principal y delega la responsabilidad de la implementación a cada sede por separado, haciendo que cada sede destine una parte de su presupuesto para esta parte, diseñando por separado sus materiales y métodos.

Este modelo se recomienda para Entidades que tienen objetivos específicos a cumplir en cada sede específica que pueden diferir un poco al ente principal, por lo que este modelo brinda dicha autonomía a cada unidad organizacional.

Una vez se determina el modelo de administración, se deben proceder a la **identificación de las necesidades de la Entidad**.

9. IDENTIFICACIÓN DE NECESIDADES

Para poder diseñar el plan apropiadamente, deben identificarse las necesidades dentro de la Entidad, el resultado de identificar estas necesidades, es la justificación que se tendrá para implementar el plan.

Es clave involucrar en el hallazgo de dichas necesidades a todo el personal, la siguiente clasificación de roles, podría ayudar a identificarlas en toda la Entidad y cada rol tendría diferentes objetivos especiales de conocimiento:

EJECUTIVOS	Deben conocer y entender las leyes y directivas que forman la base del programa de seguridad, también deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás unidades.
PERSONAL DE SEGURIDAD (OFICIALES DE SEGURIDAD)	Son los asesores expertos en seguridad, deben estar bien preparados en políticas de seguridad y buenas prácticas
DUEÑOS DE SISTEMAS	Deben entender bien las políticas de seguridad, así como también conocer sobre los controles de seguridad y la relación que tienen con los sistemas que manejan.
ADMINISTRADORES DE SISTEMAS Y PERSONAL DE SOPORTE	Estos funcionarios deben tener un buen nivel de preparación a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del Entidad de manera apropiada.
USUARIOS FINALES	Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas que tienen a disposición.

Tabla 1. Roles Y Necesidades En Capacitación Más Comunes

Es posible definir mayor o menor cantidad de roles clave dependiendo de la estructura organizacional.

9.1. MÉTODOS PARA IDENTIFICACIÓN DE NECESIDADES:

A parte de la definición de roles vista anteriormente, es posible emplear más métodos para encontrar más información de necesidades o debilidades en la institución.

Es muy importante emplear estos métodos de tal manera que permitan generan **MÉTRICAS** (*ver Guía De Indicadores De Gestión*)**,** estos resultados que se obtengan, después podrían ser comparados con una nueva medición en la etapa de desempeño que permitan generar a su vez un indicador del desempeño del plan de capacitación, los métodos para identificación de necesidades son los siguientes:

- Entrevistas con grupos clave o usuarios que hagan parte de los roles definidos previamente.
- Encuestas organizacionales.
- Procedimientos de ingeniería social en diferentes niveles.
- Verificar comportamientos generales del personal (sesiones abiertas, escritorios limpios etc…)
- Verificación de **los incidentes de seguridad de la información**, son una fuente muy importante para identificar vulnerabilidades y amenazas en el sistema. Dependiendo de las causas raíces que se identifiquen, se puede obtener información para determinar si es necesario capacitar o para sensibilizar a la población con base a la información obtenida.
- Análisis de eventos en los dispositivos de seguridad (firewall, IDS/IPS, sistemas SIEM) o intrusiones en páginas web.
- Tendencias en el sector donde se desempeña la Entidad.

A continuación se da un ejemplo donde se emplea uno de los métodos anteriores y se genera una MÉTRICA.

EJEMPLO:

Se toma una muestra de 20 usuarios de toda la Entidad y se procede a realizar un procedimiento de ingeniería social con cada uno de ellos (se intentan obtener sus contraseñas vía telefónica), al finalizar las pruebas, 15 de los usuarios hicieron entrega de su contraseña. Esto indica que un **75%** fue víctima del ataque y **permite concluir que hay desconocimiento sobre el buen uso de las contraseñas**.

Con la prueba anterior se encontró una necesidad (un tema para sensibilizar) y una métrica.

Posteriormente, después de implementar el plan de capacitación, se puede aplicar una nueva prueba del mismo tipo y se puede hacer una comparación de resultados, esperando que dicho porcentaje baje. Así se podría medir la efectividad del plan.

El uso de los métodos previos deberá permitir responder las siguientes preguntas:

Figura 3. Preguntas Clave Para Identificar Necesidades En Capacitación

9.2. COLABORACIÓN CON OTRAS ÁREAS Y ALGUNAS NECESIDADES ADICIONALES A IDENTIFICAR:

El área de recursos humanos puede ser de gran ayuda para identificar otros requisitos, como personal con discapacidad y áreas adecuadas para dictar capacitaciones de tipo presencial, así como también dependiendo del tipo de métodos a utilizar, pueden requerirse recursos de sistemas o del área de TI, que deberán gestionarse con anticipación.

10. DISEÑO DEL PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN:

Una vez se identifican todas las necesidades, se debe proceder con la elaboración del **documento maestro que es el plan en sí**, el cuál debe contener los siguientes elementos (*se presentará a la alta gerencia en la fase III*).

1. Políticas para que se ejecute un plan de capacitación y sensibilización, que deberán estar incluidas en la política de seguridad de la información (Ver *guía de Implementación de políticas de seguridad de la información*).
2. El alcance del programa.
3. Roles y responsabilidades de quienes diseñaran, desarrollaran, implementarán y mejorarán continuamente el programa y el material.
4. Metas a cumplir con el programa desarrollado.
5. Audiencias objetivo para cada aspecto, quienes deben ser sensibilizados, quienes capacitados o entrenados.
6. Cursos obligatorios para todo el personal.
7. Temas a ser tocados en cada sesión o cada curso.
8. Métodos a desplegar para brindar las capacitaciones respectivas.
9. Frecuencia de las capacitaciones o las situaciones en las que será necesaria una capacitación (reinducciones o capacitaciones para personal nuevo etc….).
10. Documentación y evidencia de cada aspecto del programa (incluyendo evaluaciones).
11. Evaluación y renovación del material creado.

10.1. DEFINIR PRIORIDADES:

Una vez armado el documento completo, es necesario definir las prioridades que tendrá el programa, dichas prioridades pueden ser contempladas con base a los siguientes aspectos:

DISPONIBILIDAD DE RECURSOS/MATERIALES
• Si hay presupuesto disponible sin ningún problema, es posible iniciar con los aspectos más claves que se consideren, sin embargo, se debe contemplar tiempos de desarrollo de material y/o instructores.
IMPACTO EN LA ORGANIZACIÓN
• Dependiendo del rol o impacto de ciertos cargos en la organización, puede ser necesario dar prioridad a la capacitación o sensibilización a cierta población.
NECESIDADES CRÍTICAS DE PROYECTOS
• Por ejemplo, para poder, desplegar un nuevo sistema operativo, es necesario realizar una capacitación a todos los usuarios previo al despliegue.
ESTADO ACTUAL DEL PLAN (BRECHAS)
• Brechas o falencias que se hayan identificado en el plan y que se necesiten corregir.

Tabla 2. Definición De Prioridades Para Capacitación

10.2. DEFINIR LA COMPLEJIDAD DEL MATERIAL A DESARROLLAR / ADQUIRIR / EMPLEAR:

La decisión de que tan complejo será el material a desarrollar/adquirir/emplear debe estar definido por el rol y/o responsabilidad de los diferentes grupos de usuarios dentro de la Entidad.

Es importante diferenciar que un material de sensibilización no debe tener el mismo grado de complejidad que un material de entrenamiento, ya que el entrenamiento busca que el usuario después de ser entrenado adquiera unas habilidades específicas para sus labores, mientras que el material de sensibilización busca disuadir a los usuarios a comportarse de determinada manera, para evitar consecuencias tanto para él, como para la Entidad.

10.3. FINANCIAMIENTO DEL PLAN DE CAPACITACIONES:

Después de definir prioridades y el plan a desarrollar. Se debe realizar el estimado de recursos financieros necesario para desarrollar el plan. La idea es enviar un mensaje claro a la alta dirección de que de ahora en adelante debe existir un presupuesto (rubro) definido para desarrollar los planes de capacitación. Dicho informe debería incluir las siguientes características:

1. Presupuesto total aproximado destinado a la formación del personal (aproximado).

2. Por cada rol o grupo de usuarios, cuanto se destinaría (ya que pagar cursos de certificación a ingenieros no cuesta lo mismo que capacitar usuarios finales en buenas prácticas).
3. Porcentaje del total del presupuesto de IT que iría a formación (para mostrar cuanto se destinará del gran total).

Adicionalmente, es bueno indicar que las áreas deben priorizar este aspecto de formación, para que el programa se desarrolle a plenitud.

11. DESARROLLO DE MATERIALES PARA EL PROGRAMA

El desarrollo/adquisición/recopilación de los materiales debe basarse en 2 **premisas**:

1. ¿Qué comportamiento se desea reforzar? (Sensibilización)
2. ¿Qué habilidades es necesario que sean aprendidas y aplicadas por los usuarios? (Entrenamiento)

Otra consideración importante, es que se vea el énfasis en el desarrollo del material para grupo de interés, es decir, que no sea un material genérico empleado para todo el mundo, porque esto puede derivar en desinterés por parte de los usuarios y pueden ignorar las sesiones.

11.1. DESARROLLO DE MATERIAL PARA SENSIBILIZACIÓN:

Cabe aclarar que la sensibilización es algo que aplicará para toda la Entidad por igual. Todos los empleados deben ver la información entregada de sensibilización como una responsabilidad compartida en seguridad de la información y que todos son importantes en esa labor.

Ahora, basta con preguntar ¿Qué quiere la Entidad que todos y cada uno de sus miembros sepa sobre seguridad de la información?. Entre los temas más importantes de sensibilización se encuentran los siguientes, aunque de acuerdo a las necesidades identificadas puede variar la cantidad:

Administración De Contraseñas	Uso Y Manejo De Inventario
Malware y sus diferentes tipos	Software Permitido/Prohibido En La Entidad
Políticas Organizacionales Relacionadas Con Seguridad De La Información	Uso De Dispositivos De La Entidad Fuera De Las Instalaciones
Uso De Correo Electrónico E Identificación De Correos Sospechosos	Seguridad En El Puesto De Trabajo
Uso Apropiado De Internet	Temas de control de acceso a los sistemas (privilegios, separación de roles)
Política De Escritorio Limpio	**Ingeniería Social**
Sanciones Por Incumplimiento De Las Políticas	**Gestión De Incidentes (Como reportar, que puedo reportar)**

Spam	"Shoulder Surfing"
Backups Y Recuperación	Cambios En Los Sistemas
Amenazas Y Vulnerabilidades Comunes	Roles Y Responsabilidades En La Entidad

Tabla 3. Temáticas Para Sensibilización Del Personal En Seguridad De La Información

Se puede disponer de material diverso para sensibilización desde varias fuentes como:

- Organizaciones profesionales y proveedores de seguridad de la información.
- Periódicos.
- Conferencias de seguridad, seminarios online (Que generan memorias o presentaciones que pueden ser útiles).
- Newsfeed o boletines sobre seguridad en sitios web.

Toda esta información o material de sensibilización puede ser presentada por temas separados o en sesiones únicas (que incluyan varios temas) a través de un instructor. Las técnicas de comunicación del material a los usuarios se tratan en la siguiente fase del plan (*Ver Fase III. Técnicas Recomendadas Para Comunicación De Información De Sensibilización*).

11.2. DESARROLLO DE MATERIAL PARA ENTRENAMIENTO:

En la segunda premisa se habla de “Que habilidades necesito que los usuarios adquieran”, esto indica que deben identificarse los grupos que requieren el entrenamiento (generalmente es el personal de TI) o en casos especiales puede requerirse entrenar a todos los usuarios en el uso de un nuevo sistema.

Para desarrollar el material de entrenamiento pueden emplearse los siguientes métodos (debe considerarse una relación de costo-beneficio con cada uno):

- Pueden contratarse proveedores relacionados con la necesidad identificada (dependiendo de la plataforma o de la necesidad específica).
- Puede utilizarse material de internet, suscripción a plataformas de e-learning que dictan cursos de capacitación, MOOCS etc…
- Búsqueda de convenios interinstitucionales con ICETEX o SENA para entrenar al personal de TI (lo que puede representar una reducción de costos en este aspecto).
- Para diseñar cursos de entrenamiento inhouse (desarrollados internamente), pueden utilizarse metodologías como la NIST 800-16, que define varios roles de TI y permiten dar un enfoque de enseñanza a cada rol.

Los diferentes tipos de difusión de este material de entrenamiento, se tratan en la siguiente fase del plan (*Ver Fase III. Técnicas Recomendadas Para Comunicación De Información De Sensibilización*).

Una vez se seleccionan los materiales a desarrollar/adquirir, se finaliza el documento maestro y se deberá presentar a la alta dirección, para aprobación.

12. IMPLEMENTACIÓN DEL PROGRAMA

12.1. SOCIALIZACIÓN DEL PLAN CON LA ALTA DIRECCIÓN:

Lo primero que debe hacerse es socializar el programa que se diseñó en las fases anteriores, para así asegurar el apoyo y los recursos necesarios por parte de la gerencia para la ejecución. Dependiendo del modelo de administración escogido en la **FASE I**, la comunicación del plan se hará en el ente central a la gerencia, a los subgerentes asignados en cada unidad organizacional etc… según corresponda a cada modelo.

Una vez se logra la aprobación por parte de la alta dirección, la implementación puede dar inicio (desarrollando o contratando los materiales propuestos para cada fin). A continuación se definen técnicas que permiten difundir o comunicar la información.

12.2. TÉCNICAS RECOMENDADAS PARA COMUNICACIÓN DE INFORMACIÓN DE SENSIBILIZACIÓN

Hay a disposición muchas técnicas para la propagación de mensajes de sensibilización, la selección de cada método debe ser acorde a los recursos y tecnología a disposición, algunos ejemplos son:

- 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).

Por lo general, los mensajes de sensibilización son de mucha brevedad y simplicidad, lo que facilita en gran medida la recepción del mensaje que se está transmitiendo. El uso de imágenes o videos pueden reforzar el tema a tratar.

12.3. TÉCNICAS RECOMENDADAS PARA LA COMUNICACIÓN DE MATERIAL DE ENTRENAMIENTO

Las técnicas para entrenamiento deben aprovechar al máximo los avances tecnológicos, empleando sistemas que brinden facilidad de uso y acceso, escalabilidad y que sean ofrecidas por varios proveedores en la industria.

Dentro de las técnicas más comunes y efectivas son las siguientes:

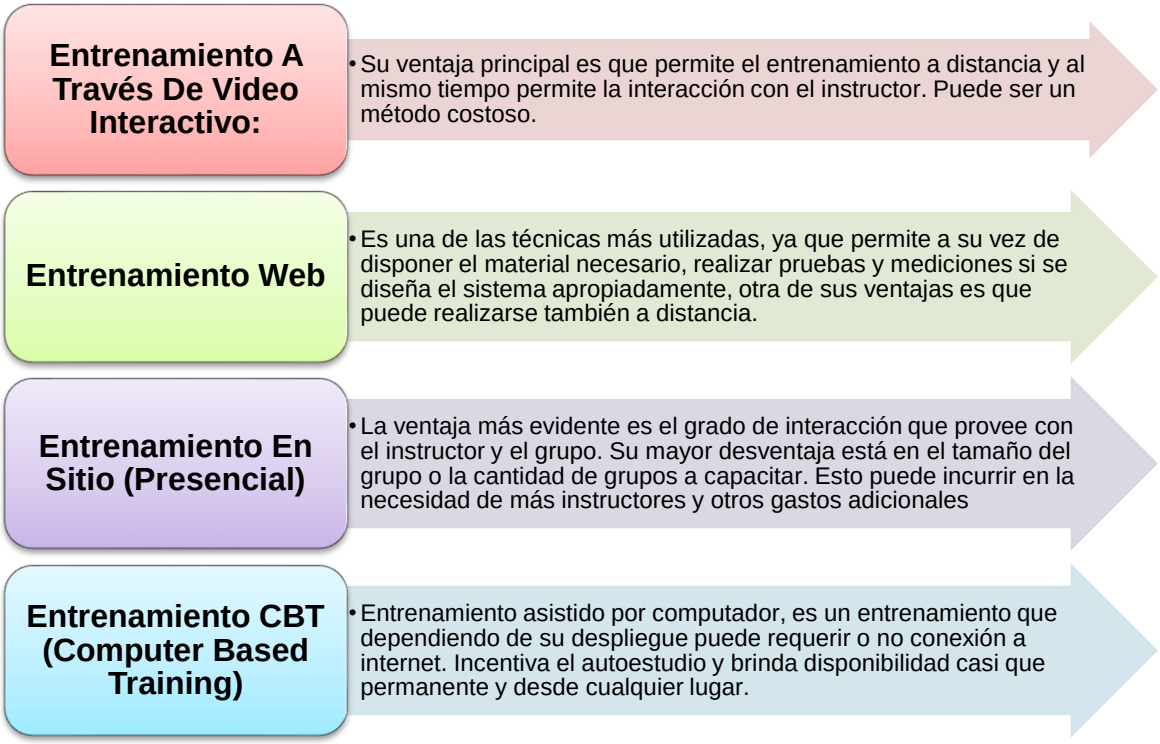

Figura 4. Técnicas Para Comunicación De Información

Dependiendo de los recursos a disposición, pueden emplearse varios de estos tipos a la vez, ya que cada uno ofrece ventajas significativas.

12.4. EVIDENCIAS DE LA ASISTENCIA A CAPACITACIONES Y EL COMPROMISO CON LA ENTIDAD:

Es importante mencionar que cuando los usuarios reciban las sesiones de sensibilización o entrenamiento, certifiquen su asistencia y asuman sus respectivos compromisos con la preservación de la seguridad de la información en la Entidad (con las políticas de seguridad de la compañía).

Esto puede realizarse a través de formatos de asistencias a las capacitaciones, con cláusulas que indiquen que han recibido el entrenamiento y sensibilización sobre los temas determinados sobre seguridad de la información.

Esta evidencia puede servir para justificar algún tipo de sanción a comportamientos inadecuados o incumplimiento a las políticas de seguridad.

13. POST-IMPLEMENTACIÓN (EVALUACIÓN Y MEJORAMIENTO CONTINUO DEL PROGRAMA).

13.1. MONITOREO DEL PLAN DE CAPACITACIONES:

Es bueno llevar registros y controles sobre cómo se desenvuelve el programa de capacitaciones, esto se puede realizar a través de alguna plataforma que permita manejar cronogramas, cargar los soportes de asistencia etc… Y que a su vez permita generar reportes de alto nivel para mostrar progresos y otros tipos de datos a nivel gerencial.

El orden y buena planificación asegurarán el buen desarrollo de las actividades.

Además esta plataforma podría ayudar a generar las encuestas para los usuarios para recolectar la información necesaria para generar MÉTRICAS para el proceso de mejoramiento.

13.2. EVALUACIÓN DE LAS ACTIVIDADES DE SENSIBILIZACIÓN / ENTRENAMIENTO:

Un programa de entrenamiento, sensibilización y comunicación no podrá mejorarse, sin antes saber cómo se está desempeñando al interior de la institución, para ello, es necesario buscar métodos que nos indiquen la efectividad del programa, para así a través de **MÉTRICAS**, poder medir su eficacia y justificar cuantitativa o cualitativamente el desempeño.

Dentro de los métodos más comunes para evaluar los entrenamientos o campañas de sensibilización se encuentran (***pueden ser los mismos métodos empleados en la identificación de necesidades de la FASE I, para comparar los resultados del antes y el ahora***):

- 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.

Las MÉTRICAS obtenidas en este punto, pueden compararse con las MÉTRICAS generadas en la fase de necesidades, para así obtener un indicador de desempeño.

Esta será la base para determinar que se debe mejorar en el plan de capacitaciones.

14. MEJORAMIENTO DEL PLAN DE CAPACITACIONES:

A parte de los resultados obtenidos en la evaluación, existen otros factores que se deben tener en cuenta para el mejoramiento continuo del plan de capacitaciones, como los avances tecnológicos, nuevas amenazas y vulnerabilidades, modalidades de ingeniería social, nuevas leyes que impliquen adoptar nuevas medidas, nuevas políticas de seguridad de la compañía etc…

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.

15. INDICADORES DE UN PLAN DE CAPACITACIONES EXITOSO

Un plan podría considerarse exitoso si se manejan o se tienen los siguientes aspectos:

1. Suficientes fondos para su desarrollo y mejoramiento.
2. Una estrategia bien enfocada en los diferentes roles de la Entidad.
3. Uso de MÉTRICAS, que permitan saber si el plan está funcionando bien. Por ejemplo (porcentaje de usuarios capacitados apropiadamente, porcentaje de ataques de ingeniería social exitosos se ha reducido, porcentaje de usuarios que hayan recibido material de sensibilización etc…).
4. La alta gerencia acata las normas de seguridad de la información y no utilizan su estatus para evadirlas, esto indica un cambio significativo en la cultura de la Entidad.
5. Reconocimientos a nivel estatal por gestión ejemplar.(Por ejemplo premios Excelencia de Gobierno En Línea).
6. Motivación por parte de los impulsores de los planes para mejorar cada vez más.
7. Aumento en el reporte de incidentes de seguridad de la información y mejora en la gestión de este proceso.

16. RECOMENDACIONES GENERALES

- 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 Entidad.
- Un personal con entrenamiento adecuado, es un personal que puede responder más rápidamente a algún incidente de seguridad, que puede ayudar a contener y evadir eventos negativos de una manera más óptima y por consiguiente ayuda a disminuir los riesgos.
- La sensibilización se centra en modificar el comportamiento de las personas, mientras que el entrenamiento se basa en enseñar a realizar alguna labor específica.
- 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.
- El desarrollo de material para sensibilización es en mayor medida más sencillo de desarrollar que un material de entrenamiento, en ocasiones es más fácil contratar a un tercero para este fin, generalmente a los proveedores de las plataformas se les solicita una fase de transferencia de conocimiento o de entrenamiento para que el personal de seguridad o de TI aprenda a realizar las labores necesarias con los dispositivos.

17. BIBLIOGRAFÍA

- NIST (National Institute Of Standards And Technology) Special Publication 800-50 *Building an Information Technology Security Awareness and Training Program*.
- ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident management
- ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary
- ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements