KIT DE
CONCIENTIZACIÓN

MANUAL DE IMPLEMENTACIÓN

ANUIES - TIC
Comité de Tecnologías de la Información y Comunicaciones de la ANUIES

ANUIES

Índice

Introducción

El objetivo de este manual es orientar a las Instituciones de Educación Superior(IES) en la correcta distribución y aplicación de los distintos materiales que conforman este «Kit de concientización».

Mediante los materiales incluidos en el «Kit de concientización», serán capaces de realizar una campaña de concientización sobre la seguridad de la información en las instituciones.

Cada IES es diferente, por lo que es complejo ofrecer una guía paso a paso en la implantación de este kit; por esta razón, en este manual se ofrecerán ideas y recomendaciones de implementación y distribución de los contenidos del kit.

Siempre la decisión final de cómo utilizar los materiales, queda a criterio de la IES que descarga el «Kit de concientización».

Fases propuestas:

En el **ANEXO A** se puede consultar un cronograma detallado.
El **ANEXO B** contiene el detalle de los archivos que forman el kit.

Fase 1: Diagnóstico inicial

Duración	**5 días laborables/Prueba inicial**
Descripción	**Evaluación inicial del nivel de concientización en seguridad**

El primer paso que se llevará a cabo, será desplegar una o las dos «Pruebas iniciales» incluidas en el «Kit de concientización». El objetivo de éstas es concientizar al personal de lo vulnerables que son y que deben ser precavidos a la hora de confiar en los archivos que ejecutan y los correos que reciben.

Se plantean dos pruebas dirigidas diferentes: por correo electrónico y a través de una memoria USB. En ambos casos el archivo a utilizar será el mismo, pero no el medio.

Es importante considerar que la preparación de la «prueba dirigida» pase desapercibida para el mayor número de personas posible y que sólo algunos (los necesarios) sepan de su existencia.

Correo electrónico

El primer tipo de prueba está basada en el envío de un correo electrónico con un archivo adjunto, el cual, al ser ejecutado, muestra al usuario una página web, advirtiéndole del peligro que pudo haber tenido por lo que acaba de hacer.

Para ello, deben seguirse los siguientes pasos:

Se utilizará una cuenta de correo electrónico ficticia, cuyas características sean similares a los proporcionados de manera institucional. Ejemplos: sistemas@anuies.mx, auditoria@anuies.mx o nombre.apellido@anuies.mx.

Es posible crear la cuenta de correo para tal fin o de ser necesario, solicitarlo al proveedor del servicio. Empleando ésta cuenta, se enviará un correo electrónico en el que, mediante un pretexto previamente acordado, se pide a los usuarios que ejecuten el archivo que se adjunta en el correo electrónico.

Este correo puede enviarse a todo el personal o a un número determinado de destinatarios que «participarán» en el diagnóstico sin su previo conocimiento.

Es recomendable, para dar credibilidad al correo, que éste lleve incluido en copia (campo CC) a algún correo de personal importante de la institución (por ejemplo, el director) quien debe tener conocimiento explícito de la prueba.

El asunto o subject debe incluir el título con el que se quiere que lleguen los correos, por lo que debe ser lo más claro y creíble posible.

A continuación, se muestra un **ejemplo** del cuerpo del correo electrónico para realizar la prueba:

> Asunto: Auditoría de Seguridad Interna.
>
> Buenos días
>
> Desde el Departamento de Informática se hace llegar este correo informándole que en días posteriores se llevará a cabo una Auditoría de Seguridad en la institución. Uno de los procedimientos exige que se realicen ciertas comprobaciones en su equipo de cómputo.
>
> Derivado de lo anterior, se ha adjuntado a este correo un archivo que debe ser ejecutado en cada uno de sus equipos de trabajo, con el fin de obtener el estado de las actualizaciones de seguridad del sistema operativo y de las aplicaciones.
>
> Gracias por su colaboración.
>
> Departamento de Informática
> Nombre de la institución

Éste es un ejemplo que podría utilizarse en su institución, pero no necesariamente el mismo, por lo que se deja a su consideración la estructura y temática del correo electrónico. El objetivo del mismo es que el personal crea que el correo es legítimo, aunque no lo sea.

Es importante no olvidar adjuntar al correo el archivo para la prueba, éste debe de tener un nombre como auditoria_interna.exe o audit2018.exe u otro nombre que elija la institución, según el pretexto que se quiera utilizar, pero que sea acorde al asunto del correo.

Una vez finalizada la prueba, será necesario eliminar la cuenta de correo ficticia creada.

USB

Esta prueba está basada en la presencia del archivo ejecutable, en varias memorias USB en calidad de extraviadas, las cuales, al ser utilizadas por el personal que las encuentre y ejecutar el archivo, mostrará al usuario una página web advirtiéndole del peligro al que se expuso por lo que acaba de hacer. Para ello, deben seguirse los siguientes pasos:

- Es recomendable que el archivo de la prueba, vaya acompañado de otro tipo de contenido totalmente inofensivo, como una carpeta llamada «Fotos» y otra como «Trabajo» donde en cada una de ellas se incluyan ciertos archivos que vayan de acuerdo con el nombre de la carpeta, como imágenes descargadas de internet, documentos PDF y/o documentos Excel o Word. Junto a ellos, se ubicará el archivo de prueba, pudiendo ser renombrado por alguno atrayente para cualquier persona, como “confidencial.exe” o privado.exe”.

- El objetivo es que el personal encuentre y utilice la USB. Para ello, se deberá «dejar» la memoria en una ubicación en la que sea muy probable que alguien pueda encontrarla. Algunos de estos lugares pueden ser:

  - Un elevador
  - En la entrada principal
  - Una sala de espera o una cafetería
  - Los baños
  - Un pasillo principal
  - Un estacionamiento
  - Un salón de clase
  - Una banca en un área de descanso
  - Una sala de cómputo
  - En la biblioteca
  - Un escritorio

- Podría etiquetarse la USB con el nombre del departamento o área que estará implementando el kit para hacerla más atractiva y que el usuario, en caso de que la devuelva, tenga referencia a quién pertenece.

Es importante que el responsable de dejar las memorias USB no sea visto durante el proceso.

En caso de que el personal devuelva la USB al departamento de informática o a cualquier área administrativa, se le explicará la prueba y su finalidad, se le solicitará que no comente nada al resto de sus compañeros y se iniciará de nuevo el proceso, colocando la USB en otra ubicación concurrida.

La persona que recibe la USB deberá preguntarle al usuario si revisó el contenido de la misma o visualizó algún archivo, explicándole que su equipo posiblemente fue expuesto a un riesgo y se le indicará que hacer en esos casos. Si no la introdujo en algún equipo, felicitarlo por la decisión de devolver la USB sin haberla usado y agradecerle su participación en la prueba.

Además, para ambos casos se recomienda explicar los motivos de la prueba a los usuarios implicados, una vez que haya finalizado esta fase.

Archivo de prueba

El archivo que se emplea en ambos diagnósticos, es un programa cuya única misión es abrir el navegador del equipo o en el caso de que ya esté abierto, abre una pestaña de una página web del Comité de Tecnologías de la Información y Comunicaciones de la ANUIES, donde se expone los peligros de las acciones que acaba de realizar, así como las medidas que debe tomar para no provocar una posible infección de un código malicioso en la red institucional.

Es fundamental que el archivo sea renombrado de manera que sea atractivo para el personal, de ser posible, relacionado con la propia institución.

Este archivo NO es identificado por los antivirus como peligroso, sin embargo, al tratarse de un archivo ejecutable, es probable que el sistema operativo solicite confirmación de que se desea ejecutar. Una de las finalidades de esta prueba es observar que decide hacer el usuario en este punto. Una vez finalizada la prueba, se solicitará a los usuarios involucrados que devuelvan el dispositivo USB y que eliminen el archivo en caso de que haya sido copiado a su equipo.

Dentro de la información de descarga del kit en <<Prueba inicial>> podrá encontrar más información sobre el mismo.

Periodo de prueba

Se plantean dos periodos de prueba. Es importante hacer al menos una al principio del programa de concientización, con el objetivo de hacer ver al personal que el problema les afecta.

Es necesario medir cuantas personas han «ejecutado el archivo» y saber que grupos laborales son los más afectados.

El segundo periodo de prueba se puede realizar al terminar la fase «formativa» del Kit de concientización, es decir cuando se hayan entregado y explicado los procesos formativos al personal. En la propuesta que se hace al final de este manual, el segundo período se realizaría en torno al mes 8.

Se pueden aplicar las dos pruebas iniciales en ambos periodos o una en cada periodo. En cualquier caso, tras la segunda prueba se deberán tener registro del número de personas que «ejecutaron el archivo» para conocer la efectividad del programa de concientización.

Aviso informativo

Una vez terminada la fase de pruebas iniciales, se deberá enviar un mensaje al personal implicado, informándoles del comienzo del programa de concientización.

El mensaje puede ser similar al siguiente:

Asunto: Kit de concientización

Buenos días

A pesar de los grandes avances tecnológicos de los últimos años y la aparición de dispositivos y entornos de seguridad más rápidos, eficientes y sofisticados, está demostrado que el principal elemento para garantizar la seguridad de una institución somos todos y cada uno de nosotros. Somos, sin lugar a dudas, el elemento más importante de la tradicional cadena de seguridad.

Por este motivo, se ha iniciado un programa de concientización en materia de ciberseguridad, que incorpora múltiples recursos gráficos y elementos que irán viendo a lo largo de los próximos días.

Se ha comenzado con la simulación de un ataque, donde, si ejecutó el archivo debe de tomar conciencia de lo que ha ocurrido. Se trabajarán y aprenderán todos los aspectos a considerar para prevenir este tipo de infecciones.

Todo ello para mejorar la seguridad personal y de nuestra institución.

Gracias por su colaboración.
Departamento de Informática
Nombre de la institución

Fase 2: Distribución de posters y trípticos

Duración	1 día laboral
Descripción	Inicio de la fase de concientización de la seguridad

Después de distribuir la/las pruebas iniciales incluidas en el «kit de concientización» y de dar un tiempo considerable para que los usuarios hayan tenido la oportunidad de «enfrentarse» a dichas pruebas, se recomienda distribuir en diversas ubicaciones de la institución los posters incluidos en el «Kit de concientización».

Para ello, deberán ser impresos y colocados en lugares visibles donde el personal los pueda leer tranquilamente (el elevador, cafeterías, mamparas, bibliotecas, pasillos etc.).

Este será también el momento de imprimir y preparar los trípticos que se incluyen en el kit. Se imprimirá el número de copias que se considere necesario, para que se puedan leer de forma tranquila durante el tiempo libre, en su casa, etc.

También podrían ser publicadas las imágenes en los sitios públicos de la institución, redes sociales o enviarlos por correo electrónico de manera escalonada.

Fase 3: Proceso formativo

Duración	1 proceso formativo/2 meses Total: 8 meses
Descripción	Distribución del material de concientización de seguridad de cada proceso.

El siguiente paso es distribuir de forma organizada y estratégica los materiales incluidos dentro de cada uno de los procesos que incluye el «Kit de concientización».

En el kit se incluyen cuatro procesos (o temáticas de formación) diferentes. Cada uno de éstos, se empleará para transmitir información útil sobre seguridad de la información y consejos o buenas prácticas a la hora de manejar información institucional. Cada proceso estará enfocado en un ámbito relevante en cuanto a la seguridad de la institución, los cuales son:

- **La información:** Este proceso describe la forma de tratar la información o datos sensibles que maneja y genera la institución, desde el punto de vista de la seguridad.

- **Almacenamiento de la información:** Se dan a conocer las medidas de seguridad a considerar y aplicar en los diferentes dispositivos electrónicos que se utilizan para trabajar con información institucional, tanto dentro, como fuera de la IES.

- **El lugar de trabajo:** menciona las medidas de seguridad y buenas prácticas a considerar y aplicar en la institución, para que sea lo más segura posible.

- **Los dispositivos móviles:** describen las medidas de seguridad y buenas prácticas a tener en cuenta y a aplicar en los dispositivos móviles que se utilizan para trabajar con información institucional, tanto dentro como fuera de la IES.

Para cada uno de estos procesos se incluye el siguiente material:

- **Vídeo** que permite asimilar los consejos sobre la seguridad en la institución de forma práctica y entretenida.

- **Presentación** útil en caso de realizarse una exposición donde el ponente explique al personal la problemática y como evitarla. La presentación incluye los principales conceptos de cada proceso de formación.

- **Documento informativo** que muestra el desarrollo de los conceptos a asimilar, redactados de manera explícita y detallada, junto con ejemplos y buenas prácticas.

- **Fondos de pantalla** son imágenes que se pueden colocar en los equipos de cómputo del personal, como fondos de escritorio o como protector de pantalla de bloqueo. El contenido de éstos son consejos o recordatorios sobre la importancia de la seguridad institucional. Si se instalan como fondo de escritorio deberán ser cambiados una vez al mes para que el personal pueda aprender de los mensajes contenidos en todos ellos.

- **Evaluación del proceso** se trata de un cuestionario con diez preguntas de opción múltiple sobre cada tema.

La distribución de estos materiales puede realizarse por cada proceso formativo, es decir, por cada tema de referencia, distribuir los materiales según se explica a continuación.

Si la institución organiza cursos de capacitación, los contenidos se difundirán y mostrarán dentro del mismo, en caso contrario, se divulgarán para que el personal los lea y visualice.

En este último caso, la distribución del material, puede hacerse de diferentes formas: mediante un correo electrónico con el material adjunto, habilitar una carpeta compartida con el personal para que ingresen y sean ellos los que descarguen el material, publicarlo en la red institucional, a través de redes sociales de la IES, etc.

Inicialmente se recomienda enseñar los videos, ya que de una forma visual se va introduciendo al personal en la temática de concientización.

A continuación, se entregarán los documentos explicativos. Si la institución ha organizado cursos de capacitación, el ponente podrá utilizar las presentaciones para ir explicando de una forma detallada lo que se indica en los documentos explicativos de cada proceso formativo. Si no es posible este esquema, los documentos se distribuirán impresos, o a través de correo electrónico y se les pedirá que los lean detenidamente, ya que posteriormente se les realizará un cuestionario que deben responder.

Además, se les distribuirá a las personas los fondos de escritorio o pantallas de bloqueo, indicándoles el procedimiento para su instalación. Alternativamente este proceso lo puede realizar el personal del área o departamento de informática o TI. Lo ideal sería usar el fondo de escritorio o pantalla de bloqueo específico de la temática recién explicada, para que sirva de recordatorio continuo.

Por último y tras un periodo considerable, se le pedirá al personal involucrado que realicen un cuestionario para la evaluación del conocimiento adquirido, sobre la temática recién explicada. El Kit de concientización incluye estas evaluaciones de auto-diagnóstico por temática, la forma en que se realizarán éstos se deja abierto a la institución, ya que pueden realizarse dentro del curso de capacitación o si no es posible realizarlo, el día siguiente a la entrega de los otros materiales, para que el empleado haya tenido tiempo de asimilar los conocimientos.

Se considera conveniente dejar unos días entre la distribución de estos documentos y la distribución del siguiente material. De esta manera, se deja el tiempo suficiente para que el personal tenga la oportunidad de asimilar los contenidos y conceptos explicados.

El análisis de la evaluación permitirá evaluar el nivel de concientización en seguridad de la institución y del personal.

Fase 4: Consejos de seguridad mensuales

Duración	1 – 2 consejos / mes
Descripción	Consejos y buenas prácticas en seguridad

Como parte del «Kit de concientización», se incluyen 12 consejos de seguridad. Éstos pueden utilizarse a modo de recordatorio de los materiales y contenidos ya distribuidos.

Los consejos son imágenes que se pueden publicar en un blog interno, en la red institucional o en las redes sociales de la IES, pueden ser enviadas por correo electrónico dentro de un marco de capacitación continua, impresos o utilizados como posters. También pueden ser utilizados como nuevos fondos de escritorio o de pantalla de bloqueo. Se deja a la institución la decisión de cómo utilizar y difundir estos consejos de seguridad.

Se pueden «publicar» uno o dos consejos de seguridad cada mes, pero nunca más, porque no se debe saturar al personal con excesiva información.

Una idea opcional, es organizar alguna actividad (a criterio de la institución) que esté relacionada con el consejo que se publica cada mes. De esta manera, se consigue que el personal, además de recordar y asimilar estos consejos, se involucren y los apliquen de alguna manera práctica. Un ejemplo podría ser el premio al empleado más seguro del mes, etc.

Fase 5: Recordatorio – Evaluación final

Duración	5 días laborables
Descripción	Evaluación que permite saber el nivel de concientización en seguridad adquirida por el personal

Se considera oportuno, una vez pasados unos 6 meses de la puesta en marcha del «kit de concientización», repetir las pruebas iniciales de la Fase 1 o realizar una nueva, con el fin de que sea algo diferente para el personal. Así, si al principio de la implementación del kit se realizó la prueba inicial del correo electrónico, ahora se podría hacer el de la USB y viceversa. O se podrían lanzar de nuevo los dos tipos de diagnósticos.

Con esto se persiguen dos objetivos. El primero, que el personal recuerde los consejos de seguridad explicados mediante el material del «kit de concientización», y a nivel institucional, permitirá evaluar el impacto de dicho kit en cuanto a la concientización en seguridad de la institución y del personal. Esta fase tendrá una duración aproximada de 5 días laborales.

Fase 6: Valoración – Encuesta de satisfacción

Duración	5 minutos
Descripción	**Evaluación sobre el Kit de concientización en seguridad para la IES**

Una vez que se haya implementado el «Kit de concientización», la institución puede hacer llegar su experiencia y opinión sobre el proceso y utilidad en materia de concientización de la seguridad de la información.

Para complementar la encuesta es necesario dedicar únicamente cinco minutos, para posteriormente enviarla al Comité de Tecnologías de la Información y Comunicaciones de la ANUIES y conseguir una retroalimentación continua para mejorar el kit.

La encuesta consta de nueve aspectos a evaluar, con un valor del 1 al 5, donde el 5 corresponde a un desempeño excelente y el 1 a una utilidad deficiente.

Anexo A: Planificación de la implementación del Kit

Para una mejor comprensión sobre la correcta implementación del «kit de concientización» INCIBE propone una planificación estándar, que guiará a la institución a establecer una estimación sobre los tiempos necesarios para cada una de las fases que componen el «kit de concientización» durante el período de un año.

Las tareas incluidas en la siguiente tabla, están ordenadas de manera cronológica.

TAREA	DURACION	MES
Fase 1 – Diagnóstico inicial	5 días	Mes 1
Distribución de posters y trípticos	1 día	Mes 1
Proceso formativo: **La información**	2 días	Mes 1
Consejo de seguridad 1 y 2	1 día	Mes 1
Consejo de seguridad 3	1 día	Mes 2
Proceso formativo: **Almacenamiento de la información**	2 días	Mes 3
Consejo de seguridad 4 y 5	1 día	Mes 3
Consejo de seguridad 6	1 día	Mes 4
Proceso formativo: **El lugar de trabajo**	2 días	Mes 5
Consejo de seguridad 7 y 8	1 día	Mes 5
Consejo de seguridad 9	1 día	Mes 6
Proceso formativo: **Los dispositivos móviles**	2 días	Mes 7
Consejo de seguridad 10 y 11	1 día	Mes 7
Consejo de seguridad 12	1 día	Mes 8
Fase 5 - Recordatorio – Evaluación final	5 días	Mes 9
Encuesta de satisfacción	1 día	Mes 9

Los contenidos de un proceso formativo serían los siguientes:

TAREAS DE CADA PROCESO FORMATIVO	DURACIÓN
Distribución de video	15 min
Distribución / lectura del documento informativo	1 hora
Explicación del ponente usando la presentación	1 hora
Actualización de los fondos de escritorio o pantallas de bloqueo	15 min
Evaluación del proceso (obligatoria)	30 min

Anexo B: Contenido del kit

El kit está formado por los siguientes contenidos:

Materiales del Kit de Concientización	
Manual	Manual de implementación
Prueba inicial	• Guía para la realización de la prueba inicial (correo electrónico) dentro de la institución • Guía para la prueba inicial con USB dentro de la institución • Elemento principal de la prueba: archivo ejecutable (MD5Sum:)
Posters	• Importancia de la seguridad de la información en las organizaciones • La seguridad de la información y las personas • Todos somos seguridad informática • La ciberseguridad empieza por TI
Trípticos	• La información • Medios de almacenamiento • El lugar de trabajo • Los dispositivos móviles • *Phishing* • Decálogo sobre el uso de la información • *Bring Your Own Device* • Redes sociales
Videos	• Video 1: La información • Video 2: Almacenamiento de la información • Video 3: El lugar de trabajo • Video 4: Los dispositivos móviles

Presentaciones	• Presentación 1: La información • Presentación 2: Almacenamiento de la información • Presentación 3: El lugar de trabajo. • Presentación 4: Los dispositivos móviles
Documentos informativos	• Documento informativo 1: La información. • Documento informativo 2: Almacenamiento de la información • Documento informativo 3: El lugar de trabajo • Documento informativo 4: Los dispositivos móviles
Fondos de pantallas o pantallas de bloqueo (resolución 1280x720 y 1920x1080)	• Protege la información, estés donde estés • Cuidado con los metadatos, son unos **chivatos** • Tus dispositivos son vulnerables, protégelos. • Hora de irse, hora de guardar. • El papel confidencial no va a la papelera de reciclaje • Este equipo está bloqueado I • Este equipo está bloqueado II • ¿Tu *password* es 1234? • No te olvides de mí
Consejos	• Protección de la información • Cifrado de la información • Borrado de información segura • Uso de USB • Copias de seguridad • Documentación en papel • Contraseñas robustas • Bloqueo de sesión • Escritorios limpios • Dispositivos móviles • Uso de wifi públicas • Sentido común

Evaluaciones	- Evaluación 1: La información - Evaluación 2: Almacenamiento de la información - Evaluación 3: El lugar de trabajo - Evaluación 4: Los dispositivos móviles
Encuesta	Encuesta de satisfacción