INSTITUTO NACIONAL DE CIBERSEGURIDAD

KIT DE CONCIENCIACIÓN

MANUAL DE IMPLANTACIÓN

Índice

Introducción

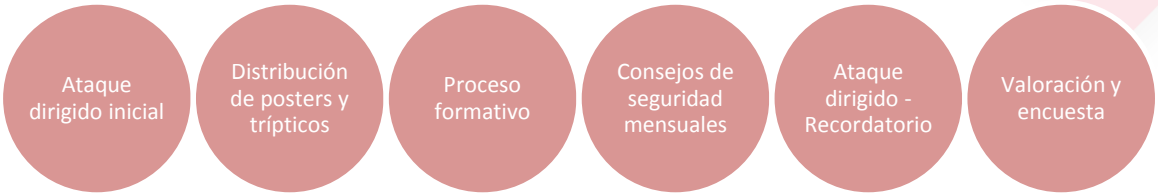
El objetivo de este manual es orientar a las empresas en la correcta distribución y aplicación de los distintos materiales que conforman este «kit de concienciación».

Mediante los materiales incluidos en el «kit de concienciación», seremos capaces de realizar una campaña de concienciación sobre seguridad de la información en nuestra empresa.

Cada sector industrial y cada empresa son diferentes, por lo que es complejo ofrecer unas reglas estrictas de implantación de este kit de concienciación. Por esta razón en este manual se ofrecerán ideas y recomendaciones de implantación y distribución de los contenidos del kit.

Siempre la decisión final de cómo utilizar los materiales queda supeditada al criterio de la empresa que descarga el «kit de concienciación».

Se propone las siguientes fases:



En el ANEXO A pueden consultar un cronograma detallado.

El ANEXO B contiene el detalle de los ficheros que forman el kit

Fase 1: Ataques dirigidos

Duración	5 días laborales/ataque
Descripción	Evaluación inicial del nivel de concienciación en seguridad

El primer paso que llevaremos a cabo, será desplegar uno o los dos «ataques dirigidos» incluidos en el «kit de concienciación». El objetivo de estos «ataques dirigidos» es concienciar a nuestros empleados de los 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 ataques dirigidos con vías de ataque diferentes: por correo electrónico o a través de una memoria USB. En ambos casos el archivo a utilizar será el mismo, pero no el medio.

Es importante intentar que la preparación del «ataque dirigido» pase desapercibida para el mayor número de empleados posible y que solo unos pocos (los necesarios) sepan de su existencia.

Correo electrónico con archivo malicioso adjunto:

El primer tipo de ataque está basado en el envío de un correo electrónico con un fichero infectado, el cual al ser ejecutado, muestra al usuario un portal Web advirtiéndole del peligro que supone lo que acaba de hacer. Para ello, deben seguirse los siguientes pasos:

Se utilizará una cuenta de correo electrónico ficticia pero cuyas características sean similares (nombre y apellidos de un empleado «nuevo» o cuenta tipo de un departamento) a las cuentas de correo de la empresa. Ejemplos: sistemas@empresa.es, auditoria@empresa.es o nombre.apellido@empresa.es.

Es posible crear la cuenta de correo para tal fin o solicitarlo a nuestro hosting. Empleando esta cuenta de correo, se enviará un correo electrónico en el que mediante un pretexto previamente pactado, se pide a las víctimas que ejecuten el archivo que se incluye en el correo electrónico.

Este correo electrónico, puede enviarse a todos los empleados o a un número determinado de destinatarios que «participarán» en el experimento sin su previo conocimiento.

Es recomendable, para dar credibilidad al correo, que éste lleve incluido en copia (campo CC) a algún cargo importante de la empresa. Antes debe obtenerse el permiso explícito de esta persona para incluirlo en la prueba.

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

A continuación, se muestra un **ejemplo** de correo electrónico a utilizar para desplegar el ataque:

> *Asunto: Auditoría de Seguridad Interna*
>
> *Buenos días,*
>
> *Desde el Departamento de Informática os hacemos llegar este correo en relación con la Auditoría de Seguridad que se está llevando a cabo actualmente en la empresa. Uno de los procedimientos exige que se realicen ciertas comprobaciones en los equipos de usuario de la red interna.*
>
> *Por ello, hemos adjuntado a este correo un fichero que debe ser ejecutado en cada uno de vuestros equipos de trabajo, con el fin de obtener el estado actual de los parches de seguridad del sistema operativo y de las actualizaciones de las aplicaciones.*
>
> *Gracias por vuestra colaboración.*
>
> *Departamento de Informática*
>
> *Empresa*

Esto es un ejemplo y puede no amoldarse a la estructura de la empresa, por lo que se deja en sus manos la estructura y temática del correo electrónico. El objetivo del mismo es que el empleado se crea que el correo es legítimo, aunque no lo sea.

Es imprescindible no olvidar adjuntar al correo a enviar el fichero infectado. Este archivo debe tener un nombre como *auditoria_interna.exe* o *audit2015.exe*, u otro nombre que elija la empresa según el pretexto que se quiera utilizar

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

Pendrive Infectado:

El ataque está basado en la presencia de un fichero infectado en varias memorias USB «extraviadas», los cuales al ser ejecutados, muestran al usuario un portal web advirtiéndole del peligro que supone lo que acaba de hacer. Para ello, deben seguirse los siguientes pasos:

1. Es recomendable que el fichero «infectado» vaya acompañado de otro tipo de contenido totalmente inofensivo como un directorio llamado «Fotos» y otro «Documentación» donde en cada uno de ellos haya ciertos ficheros genéricos como imágenes descargadas de internet, documentos PDF y/o documentos Excel o Word. Junto a ellos, se ubicará el fichero infectado, pudiendo ser renombrado con algún nombre atrayente para cualquier persona como "confidencial.exe" o "material_privado.exe".
2. El objetivo es que el usuario encuentre y utilice el USB o memoria localizada. Para ello, se deberá «abandonar» el dispositivo en una ubicación en la que sea muy probable que un usuario pueda encontrarlo. Algunos de estos lugares pueden ser:
    - ascensor
    - entrada principal
    - sala de café o comida
    - los servicios
    - pasillo transitado

    Es importante que el encargado de desplegar las memorias USB no sea detectado durante el proceso.

    En el caso de que el usuario la devuelva al departamento de Informática o cualquier otro responsable, se le explicará la prueba y su finalidad, se le solicitará que no comente nada al resto de compañeros y se iniciará de nuevo el proceso, desplegando el USB en otra ubicación.

    Es importante indicar al usuario lo correcto de su decisión de devolver el USB sin haberlo usado.

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

Archivo malicioso:

El archivo que se emplea en ambos ataques es un programa cuya única misión de este fichero es abrir el navegador de usuario o, en el caso de que ya esté abierto, abrirle una pestaña, directamente a una página web de INCIBE donde se expongan los peligros de las acciones que acaba de realizar, así como las medidas que debe tomar para no provocar una posible infección de malware en la red de la empresa.

Es fundamental que el fichero sea renombrado con un nombre «atractivo para el usuario», a ser posible relacionado con la propia empresa.

Este fichero NO es identificado por los antivirus como una amenaza. Sin embargo, al tratarse de un fichero ejecutable, es probable que el sistema operativo solicite confirmación de que se desea ejecutar. Una de las razones 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 pendrive y que eliminen el fichero en el caso de que haya sido copiado a su equipo.

Dentro de la información de descarga de los ataques dirigidos podrá encontrar más información sobre el mismo.

Periodo de despliegue

Se plantean dos periodos de despliegue de los ataques dirigidos. Es interesante lanzar al menos un ataque dirigido al principio del programa de concienciación con el objetivo de hacer ver a los empleados que el problema les afecta.

Es interesante medir cuantos empleados han «picado» y saber que grupos laborales son los más afectados.

El segundo periodo de despliegue lo podemos situar al terminar la fase «formativa» del kit de concienciación, es decir cuando se hayan entregado y explicado las píldoras informativas a los empleados. En la propuesta que hacemos al final de este manual, el segundo despliegue se realizaría en torno al mes 8.

Se pueden desplegar los dos ataques dirigidos en ambos periodos o solo uno en cada periodo. En cualquier caso, tras el segundo despliegue de los ataques dirigidos se deberán medir de nuevo las personas que «han picado» para conocer la efectividad del programa de concienciación.

Aviso informativo:

Una vez terminada la primera fase de ataques dirigidos, se deberá enviar un mensaje a los empleados informándoles del comienzo del programa de concienciación.

El mensaje puede ser similar al siguiente:

> *Asunto: Kit de sensibilización*
>
> *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 organización 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, hemos comenzado con un programa de concienciación en materia de ciberseguridad, que incorpora múltiples recursos gráficos, elementos interactivos que iremos viendo a lo largo de los próximos días.*

*Hemos comenzando con la **simulación** de un ataque simulado, dónde si habéis ejecutado el archivo habréis tomado conciencia de lo que ha ocurrido. Vamos a trabajar y aprender todos los aspectos a tener en cuenta para prevenir este tipo de ataques.*

Todo ello para mejorar nuestra seguridad desde el propio corazón de nuestra empresa: las personas.

Gracias por vuestra colaboración.

Departamento de Informática

Empresa

Fase 2: Distribución de posters y trípticos

Duración	**1 día laboral**
Descripción	Inicio de la fase de concienciación en seguridad

Después de distribuir el/los ataques dirigidos incluidos en el «kit de concienciación» y de dejar un tiempo prudencial para que los usuarios hayan tenido la oportunidad de «enfrentarse» a dichas pruebas, se recomienda distribuir en diversas ubicaciones de nuestras oficinas los **posters** incluidos en el «kit de concienciación».

Para deberán ser imprimidos y colocados en lugares visibles donde el empleado los pueda leer tranquilamente (el ascensor, la sala de café, salas de reuniones, etc.)

Este será también el momento de imprimir y preparar los trípticos que se incluyen en el kit. Se imprimirá un buen número de copias de los trípticos para que el empleado los pueda coger y leer de forma tranquila durante la pausa del café, en su casa, etc.

También puede ser interesante publicar las imágenes en la intranet o enviarlos por correo electrónico de manera escalonada.

Fase 3: Proceso formativo

Duración	**1 proceso formativo/ 2 meses. TOTAL: 8 meses**
Descripción	Distribución del grueso del material de concienciación en seguridad

El siguiente paso es distribuir de forma organizada y espaciada, los materiales incluidos dentro de cada una de las píldoras que incluye el «kit de concienciación».

En el Kit, se incluyen **cuatro píldoras** (o temáticas de formación) diferentes. Cada una de estas píldoras, se empleará para transmitir información útil sobre seguridad de la información y consejos o buenas prácticas a la hora de manejar información corporativa. Cada píldora estará enfocada en un ámbito relevante en cuanto a seguridad en la empresa se refiere:

- **La Información**: tratamiento de la información sensible que maneja y genera la empresa, desde el punto de vista de la seguridad.
- **Los soportes**: medidas de seguridad a tener en cuenta y a aplicar en los diferentes soportes que utilizamos para trabajar con información corporativa, tanto dentro como fuera de la empresa.
- **El puesto de trabajo**: medidas de seguridad y buenas prácticas a tener en cuenta y a aplicar en nuestro puesto de trabajo para que éste sea lo más seguro posible.
- **Los dispositivos móviles**: medidas de seguridad y buenas prácticas a tener en cuenta y a aplicar en los dispositivos móviles que utilizamos para trabajar con información corporativa, tanto dentro como fuera de la empresa.

Para cada una de estas píldoras se incluyen los siguientes materiales:

- **Vídeo Interactivo**: nos permite asimilar consejos sobre seguridad en la empresa de forma práctica y entretenida. Se asimila a un juego en el que se debe hacer clic en los iconos del video para que éstos revelen la información que contienen.
- **Presentación *Powerpoint***: útil sobre todo en caso de que se realice un curso de formación en el que un formador explique a los empleados la problemática y como evitarla. Las presentaciones en powerpoint Incluyen los principales conceptos a asimilar de la píldora, redactados de forma esquemática.
- **Documento *Word* explicativo**: desarrollo los conceptos a asimilar, redactados de manera explicativa y detallada, junto con ejemplos y buenas prácticas.
- **Fondos de pantalla/Salvapantallas**: se trata de unas imágenes que se pueden implantar en los equipos de escritorio de los empleados como fondos de escritorio o como salvapantallas. El contenido de éstos son consejos o recordatorios sobre la importancia de la seguridad corporativa. Si se instalan como fondo de escritorio deberán ser cambiados una vez al mes para que los empleados pueden aprender de los mensajes contenidos en todos ellos.
- **Test:** se trata de cuatro pruebas con diez preguntas de opción (respuesta simple) sobre cada temática y un test general.

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

Si la empresa ha podido organizar jornadas de formación, los siguientes contenidos se entregarán y mostrarán dentro de la jornada de formación. En caso contrario se entregarán al empleado para que los lea y visualice.

En este último caso, a la hora de distribuir un material, podemos hacerlo de diferentes formas: mediante un correo electrónico con el material adjunto; habilitar un directorio compartido al que accedan nuestros empleados y sean ellos los que se descarguen el material; publicarlo en la intranet corporativa, etc.

Inicialmente se recomienda enseñar los **videos interactivos**, ya que, de una forma entretenida va introduciendo a los empleados en materia. Estos vídeos consisten en imágenes de 360º en las que se han incluido consejos de seguridad que se visualizan después de hacer clic en los diferentes iconos que contiene la imagen para tal efecto.

A continuación se entregarán los **documentos Word** explicativos. Si la empresa ha podido organizar jornadas de formación, el instructor podrá utilizar las presentaciones **PowerPoint** para ir explicando de una forma detallada lo que se indica en los documentos explicativos de cada píldora. Si no es posible este esquema formativo, los documentos Word se entregarán o bien en mano, o bien a través de correo electrónico a los empleados y se les pedirá que los lean detenidamente, ya que posteriormente se les pasará un cuestionario que deben responder.

A continuación se les entregará a los empleados los **fondos de escritorio/salvapantallas**, indicándoles el procedimiento para su instalación. Alternativamente este proceso lo puede realizar un empleado del área de departamento de informática o TI. Lo ideal sería implantar el fondo de escritorio específico de la temática recién explicada, para que sirva de recordatorio continuo.

Por último y tras un periodo prudencial, se les pedirá a los empleados que realicen un **test** de conocimiento sobre la temática recién explicada. El kit de concienciación incluye estos tests de auto-diagnóstico por temática. La forma en que se realizarán estos test se deja abierto a la empresa, ya que pueden realizarse dentro de la jornada formativa o si no es posible realizarla, el día siguiente a la entrega de los otros materiales, para que el empleado haya tenido tiempo para asimilar los conocimientos.

Se considera conveniente dejar unos días entre la distribución de estos documentos y la distribución del siguiente material. De esta manera, dejamos tiempo suficiente para que nuestros empleados tengan la oportunidad de asimilar los contenidos y conceptos explicados.

La recogida y estudio de los tests nos permitirá evaluar el nivel de concienciación en Seguridad de nuestra empresa y empleados.

Fase 4: Consejos de seguridad mensuales

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

Como parte del «kit de concienciación», 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 el blog interno, en la intranet, pueden ser enviadas por correo electrónico dentro de un marco de formación continua. Puede ser impresas y utilizadas como posters. También pueden ser utilizadas como nuevos fondos de escritorio y/o salvapantallas. Se deja a la empresa la toma de decisión de cómo utilizar estos consejos de seguridad.

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

Una idea opcional, es organizar alguna actividad (a criterio de la empresa) que esté relacionada con el consejo que se publica cada mes. De esta manera, conseguimos que nuestros empleados, además de recordar y asimilar estos consejos, se involucren y los apliquen de alguna manera práctica. Algún ejemplo podría ser un premio al mejor puesto de trabajo, al empleado seguro del mes, etc.

Fase 5: Recordatorio – Ataques dirigidos

Duración	5 días laborales
Descripción	Evaluación final del nivel de concienciación en seguridad

Se considera oportuno, una vez pasados unos 6 meses de la puesta en marcha del «kit de concienciación», repetir las pruebas de los **ataques dirigidos** o realizar una nueva con el fin de que sea algo nuevo para los empleados. Así, si al principio del proceso formativo se realizó el ataque dirigido del correo electrónico, ahora se podría hacer el del pendrive y viceversa. O se podrían lanzar de nuevo los dos ataques.

Con esto conseguimos dos objetivos. El primero, que nuestros empleados recuerden los consejos de seguridad explicados mediante el material del «kit de concienciación», y a nivel corporativo, nos permite evaluar el impacto de dicho Kit en cuanto a la concienciación en Seguridad de nuestra empresa y empleados. Esta fase tendrá una duración aproximada de 5 días laborales.

Fase 6: Valoración - Encuesta de Satisfacción

Duración	5 minutos
Descripción	Valoración sobre el kit de concienciación en seguridad

Una vez se haya implantado el «kit de concienciación», la empresa puede hacernos llegar su experiencia y opinión sobre el proceso de implantación y su utilidad en materia de concienciación de la seguridad de la información.

Invirtiendo cinco minutos en cumplimentar dicha encuesta y enviarla a INCIBE, conseguimos una retroalimentación de información continua y una base sobre la que mejorar nuestro Kit.

La encuesta consta de nueve aspectos a evaluar, con un valor del 1 al 5, donde el 5 se corresponde con la mejor valoración.

Anexo A: Planificación implantación del Kit

Para una mejor comprensión sobre la correcta implantación del «kit de concienciación» desarrollado por INCIBE, se ha elaborado una **propuesta** planificación estándar a título orientativo que guiará al empresario a establecer una estimación sobre los tiempos necesarios de implantación de cada una de las fases que componen el «kit de concienciación» durante el periodo de un año.

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

TAREA	DURACION	MES
1. er Ataque dirigido o 1er y 2º Ataques dirigidos	5 días	Mes 1
Distribución de posters y trípticos	1 día	Mes 1
Proceso Formativo Píldora 1: **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 Píldora 2: **Los soportes**	2 días	Mes 3
Consejo de seguridad 4 y 5	1 día	Mes 3
Consejo de seguridad 6	1 día	Mes 4
Proceso Formativo Píldora 3: **El puesto 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 Píldora 4: **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
2. º Ataque dirigido o recordatorio	5 días	Mes 9
Encuesta de valoración	1 día	Mes 9

Los contenidos de un proceso formativo serían los siguientes:

TAREAS del PROCESO FORMATIVO de cada PILDORA	Duración
Entrega de video de la píldora	15 min
Entrega / lectura del documento de texto	1 hora
Explicación usando el PPT	1 hora
Actualización de los fondos de escritorio	15 min
Prueba tipo test (obligatoria)	30 min

Anexo B: Contenidos del Kit

El kit está formado por los siguientes contenidos:

Materiales del Kit de Concienciación	
Manual	Manual de implantación
Ataques dirigidos	Guía para la realización del ataque simulado (correo electrónico) dentro de la empresa Guía para la realización del ataque simulado (USB) dentro de la empresa Elemento principal del ataque: archivo del ataque simulado (MD5Sum: 6d84ae97875a4deb5ea34ed014c13c28)
Pósteres (en formato A2 y A3)	Importancia seguridad de la información en las organizaciones La seguridad de la información y las personas Todos somos ciberseguridad La ciberseguridad empieza por TI
Trípticos	La información Los soportes El puesto de trabajo Los dispositivos móviles *Phishing* Puntos clave en ciberseguridad *Bring Your Own Device* Redes sociales
Píldoras	Píldora interactiva 1: La información Píldora interactiva 2: Los soportes Píldora interactiva 3: El puesto de trabajo Píldora interactiva 4: Los dispositivos móviles
Presentaciones	Presentación 1: La información. Presentación 2: Los soportes. Presentación 3: El puesto de trabajo. Presentación 4: Los dispositivos móviles

Documentos explicativos	Documento explicativo 1: La información. Documento explicativo 2: Los soportes Documento explicativo 3: El puesto de trabajo Documento explicativo 4: Los dispositivos móviles
Salvapantallas (resolución 1280x720 y 1920x1080)	Protege la información, estés donde estés Cuidado con los metadatos, son unos chivatos Tus soportes son vulnerables, protégelos Hora de irse, hora de guardar El papel confidencial no va a la papelera 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 Mesas limpias Dispositivos móviles Uso de wifi públicas Sentido común
Test	Test 1: La información Test 2: Los soportes Test 3: El puesto de trabajo Test 4: Los dispositivos móviles
Encuesta	Encuesta de satisfacción