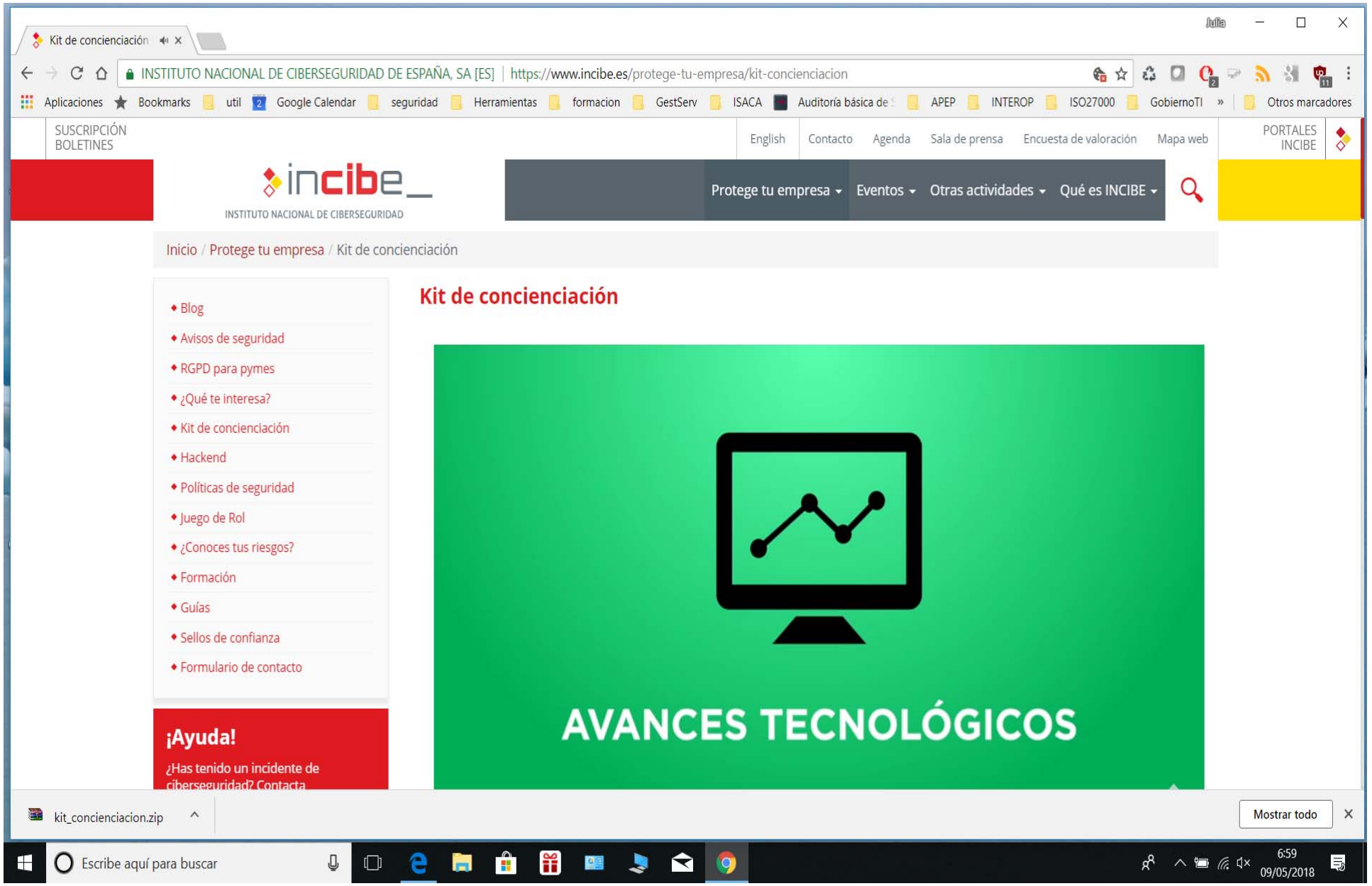
Adaptación del Kit de Concienciación de INCIBE a Universidades


Kit de concienciación
INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, SA [ES] | https://www.incibe.es/protege-tu-empresa/kit-concienciacion
SUSCRIPCIÓN BOLETINES
English
Contacto
Agenda
Sala de prensa
Encuesta de valoración
Mapa web
PORTALES INCIBE
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
Protege tu empresa
Eventos
Otras actividades
Qué es INCIBE
Inicio / Protege tu empresa / Kit de concienciación
Blog
Avisos de seguridad
RGPD para pymes
¿Qué te interesa?
Kit de concienciación
Hackend
Políticas de seguridad
Juego de Rol
¿Conoces tus riesgos?
Formación
Guías
Sellos de confianza
Formulario de contacto
¡Ayuda!
¿Has tenido un incidente de ciberseguridad? Contacta
Kit de concienciación
AVANCES TECNOLÓGICOS
kit_concienciacion.zip
Mostrar todo
Escribe aquí para buscar
6:59
09/05/2018

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Consejo del Mes

Tríptico informativo

EL PHISHING es una forma de ingeniería social en la cual un atacante intenta de forma fraudulenta adquirir información confidencial de una víctima, haciéndose pasar por un "tercero de confianza". Este tipo de ataques se han convertido en una de las amenazas externas que más acechan a las empresas.

LOS RIESGOS derivados de estas técnicas son el robo de identidad y datos confidenciales, pérdida de productividad y consumo de recursos de las redes corporativas. Los métodos utilizados para la realización del **PHISHING** no se limitan exclusivamente al correo electrónico, sino que también utilizan SMS (**SMISHING**), telefonía IP (**VISHING**), **REDES SOCIALES, MENSAJERÍA INSTANTÁNEA A TRAVÉS DEL MÓVIL, ETC.**

Para evitar estos riesgos es recomendable adoptar unas buenas prácticas principalmente en **EL USO DEL CORREO ELECTRÓNICO CORPORATIVO.**

APRENDE a identificar correctamente los correos electrónicos sospechosos de ser phishing, en general mensajes que solicitan información confidencial

VERIFICA la fuente de información de tus **CORREOS ENTRANTES.** Tu banco no te va a solicitar tus datos o claves bancarias a través del correo electrónico.

EN LUGAR DE UTILIZAR LOS ENLACES incluidos en los correos electrónicos, escribe la dirección directamente en el navegador.

Mantén **ACTUALIZADO TU EQUIPO** y todas las aplicaciones, sobre todo el antivirus y anti-spam. Aplica los parches de seguridad facilitados por los fabricantes.

Antes de introducir información confidencial en una página web, **ASEGÚRATE QUE ES SEGURA.** Han de empezar con <<https://>> y tener un candado cerrado en el navegador.

El **SMISHING** se realiza a través un

El **VISHING** se realiza a través de una llamada telefónica que simula proceder de una entidad bancaria solicitándote verificar una serie de datos.

Descripción del kit de concienciación (I)

El Kit se organiza en cuatro bloques temáticos:

- ✓ La información: tratamiento de la información sensible que maneja y genera la organización 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 organización.
- ✓ 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 organización.

Descripción del kit de concienciación (II)

Cada bloque temático incluye los siguientes materiales:

- ✓ **Vídeo Interactivo**: similar 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***: incluye los principales conceptos a asimilar del bloque temático, redactados de forma esquemática.
- ✓ **Documento *Word/PDF* explicativo**: desarrolla los conceptos con ejemplos y buenas prácticas.
- ✓ **Fondos de pantalla/Salvapantallas**: imágenes para los escritorios de los empleados.
- ✓ **Test de evaluación:** se trata de una prueba por módulo con diez preguntas de opción (respuesta simple) sobre cada temática.

Descripción del kit de concienciación (III)

Además de los contenidos de cada bloque temático el kit incluye:

- ✓ **Manual de implantación del kit:** tiene como objetivo orientar en la correcta distribución y aplicación de los materiales del kit para realizar una campaña de concienciación.
- ✓ **Ataques dirigidos:** su objetivo es concienciar a los trabajadores de su vulnerabilidad.
- ✓ **Posters y trípticos:** INCIBE recomienda usarlos al inicio de la fase de concienciación.
- ✓ **Consejos de seguridad mensuales:** consejos y buenas prácticas en seguridad que pueden utilizarse a modo de recordatorio de los materiales y contenidos de los bloques temáticos.

Manual de implantación

- ✓ Nos orienta para la elaboración de una campaña de concienciación sobre seguridad de la información en nuestra organización.
- ✓ Es complejo ofrecer unas reglas estrictas de implantación del kit de concienciación, por lo que el manual ofrece ideas y recomendaciones de implantación y distribución de los contenidos del kit.
- ✓ Propone las siguientes fases:

- ✓ Adjunta un anexo con el cronograma detallado que propone la implantación del kit durante el periodo de un año.

Subgrupo de Seguridad de CRUE-TIC

- ✓ El anexo II del ENS contiene un listado de las medidas de seguridad que deben cumplir los SI en función de su categoría.
- ✓ ENS la establece como obligatoria la Concienciación de las personas, incluso para los sistemas de nivel BAJO (mp.per.3).
- ✓ Surge la propuesta de solicitud de los fuentes del kit a INCIBE para que cada Universidad pueda adecuarla a su entorno
- ✓ Se promueve la firma de un convenio de colaboración CRUE-INCIBE

Convenio marco colaboración INCIBE-CRUE

Se firma el 22 de junio de 2016

- ✓ **Objeto:** desarrollo de actuaciones de promoción de la ciberseguridad en el ámbito de las universidades españolas.

- ✓ **Naturaleza:** administrativa. Se regula por lo establecido en el propio convenio, quedando excluido del ámbito de aplicación de la Ley de Contratos del Sector Público.

- ✓ **Recoge:** actuaciones de INCIBE y compromisos de CRUE para la colaboración en el diseño y organización de jornadas, seminarios y talleres de ciberseguridad, de común interés para ambos.

Kit de Concienciación de INCIBE

"El INCIBE pondrá a disposición de la CRUE los materiales de ciberseguridad que elabora y publica en la sección "Protege tu empresa" de su página web www.incibe.es"

- ✓ Se establecen las condiciones de uso del kit con INCIBE
- ✓ Se establece un procedimiento para la distribución de los fuentes a Universidades
- ✓ Se difunde la información sobre el procedimiento de solicitud de fuentes del kit y las condiciones de uso a la lista de Responsables de Seguridad
- ✓ Se encarga de la gestión del procedimiento la Universidad de Sevilla

Condiciones de uso

- ✓ Los materiales del kit podrán ser personalizados para el entorno universitario pero en ningún caso se eliminarán los logotipos existentes en ellos.
- ✓ Se citará la autoría de este kit (INCIBE) cuando se difundan los contenidos, ya sean originales o modificados por la universidad.
- ✓ INCIBE validará los materiales modificados antes de su distribución.
- ✓ La universidad que haga uso de los materiales proporcionará datos sobre el uso de los mismos al subgrupo de Seguridad a fin de elaborar un informe anual que se remitirá a INCIBE.
- ✓ La Universidad que haga uso de los materiales cumplimentará la encuesta que, al respecto, INCIBE publica en su web.

Solicitud de los fuentes

- ✓ Los fuentes puede solicitarlos cualquier Universidad a través de su Responsable de Seguridad siempre que esté registrado como tal en CRUETIC.

- ✓ Se solicitan mediante envío de correo electrónico a la Universidad de Sevilla (julia@us.es) con copia al entonces coordinador del subgrupo de Seguridad (joseantonio.pizarro@usc.es) y ahora al nuevo coordinador (paco.sampalo@uah.es)

- ✓ La Universidad de Sevilla facilitará los materiales a través de la consigna de la US (https://consigna.us.es)

- ✓ El solicitante es responsable de la no difusión de los fuentes.

- ✓ Cada universidad podrá adecuar los materiales en función de sus intereses.

Iniciativa: adecuación conjunta del kit

- ✓ Si todas las Universidades van a hacer cambios similares multiplicaremos nuestro trabajo y el de INCIBE, que tendrá que dar el visto bueno a las modificaciones de cada universidad.
- ✓ Se plantea la posibilidad de buscar un grupo de universidades voluntarias para decidir los cambios que debemos hacer y aplicarlos a los fuentes.
- ✓ En el mes de mayo de 2017 se organiza una videosesión a través de RedIris con doble objetivo:
  - Dar a conocer el convenio CRUE-INCIBE y el kit a las universidades
  - Anunciar la iniciativa de adecuación de los materiales del kit a universidades de forma conjunta

Iniciativa: adecuación conjunta del kit

Objetivo: elaborar un kit genérico preparado para su uso en el ámbito universitario sin necesidad de hacer cambios

- ✓ Se consensúan los cambios a los textos, los posibles cambios de imagen, los mensajes que se eliminan o los que se añaden
- ✓ Se aplican los cambios sobre los fuentes y se generan los ejecutables
- ✓ Se respetan los logos de INCIBE pero se añaden logos genéricos de CRUE
- ✓ Se solicita la validación de cambios a INCIBE con la premisa de que las Universidades que dispongan de los programas necesarios para modificar los fuentes puedan incorporar además su propio logo y algún cambio muy puntual

Iniciativa: Universidades participantes

- ✓ Universidad de Málaga
- ✓ Universidad Carlos III de Madrid
- ✓ Universidad Politécnica de Cartagena
- ✓ Universidad Complutense de Madrid
- ✓ Universidad de Educación a Distancia
- ✓ Universidad Da Coruña
- ✓ Universidad de Granada
- ✓ Universidad de Zaragoza
- ✓ Universidad de Barcelona
- ✓ Universidad Politécnica de Madrid
- ✓ Universidad de Sevilla (Coordina la iniciativa)
- ✓ Universidad de Santiago de Compostela (Contacto con INCIBE)
- ✓ IE Universidad (colabora en la traducción de materiales a inglés)

Trabajo en grupo

Herramientas utilizadas:

- ✓ Intercambio de ficheros y repositorio de documentación: *Sharepoint* de Office 365 configurado por la Universidad de Barcelona.
- ✓ Comunicación directa por correo entre los componentes del grupo.
- ✓ Convocatoria de reuniones con Doodle: reuniones mensuales para planificar el trabajo del mes
- ✓ Celebración de reuniones en la herramienta Collaborate de blackboard de la Universidad de Sevilla salav.us.es
- ✓ Excel con propuestas de cambios por parte de todas las universidades, votaciones a los cambios y resultados consensuados

Trabajo inicial

- ✓ Limpieza del kit de INCIBE para empezar a trabajar con una copia buena: eliminar lo duplicado y renombrar los ficheros para que coincidan fuente y ejecutable.

- ✓ Decidir los bloques temáticos de kit: se mantienen los cuatro bloques propuesto por INCIBE.

- ✓ Formato de los fuentes y aplicaciones a usar: .doc, .docx, .ptt y .pttx (Office), .psd (Photoshop, gimp), .ai (Adobe Illustrator o Inkscape), .indd (Adobe Indesign, Scribus con EPS generados con la versión de prueba de InDesign), .fw.png (Fireworks)

- ✓ Traducciones: a inglés (sólo dos trípticos - Universidad IE) y a catalán (completo – UB)

Adecuación por fases

Fase I: propuestas de cambios, votaciones y consenso para gráficos, trípticos, píldoras y manual, aplicación y encuesta.

- ✓ Envío de hoja excel con propuesta inicial de cambios a los materiales (US) con fecha de aportación de propuestas de otras universidades
- ✓ Recopilación en un solo excel de las propuestas y envío para votación a todas las Universidades
- ✓ Recopilación de votos para obtener cambios definitivos consensuados

Fase II: aplicación de cambios a los materiales

- ✓ Cambios de los textos
- ✓ Incluir logos de CRUETIC

Hitos de la iniciativa

Jun2016	Firma convenio INCIBE-CRUE
May2017	Videoconferencia en RedIris para organizar la iniciativa
Jun2017	Comienza el trabajo del grupo
Oct2017	Presentación del estado de la iniciativa an CRUE
Oct2017	Fin de la adecuación de los materiales y envío a para su validación
Nov2017	Visto bueno de INCIBE a la adecuación
Dic2017	Difusión del kit para Universidades a los Responsables de Seguridad
May2018	Presentación del trabajo en las Jornadas de RedIris

Encuesta de satisfacción

- ✓ El INCIBE pide a las Universidades que le hagan llegar su experiencia y opinión sobre el proceso de implantación y su utilidad en materia de concienciación de la seguridad de la información.

- ✓ INCIBE utilizará los datos de las encuestas como retroalimentación de información continua y base sobre la que mejorar el Kit.

- ✓ En el acuerdo con la CRUE, las universidades nos comprometemos, además de enviar la encuesta a enviar un informe sobre el uso dado a los materiales.

Posibles mejoras

✓Traducción completa a inglés

✓Cursos Online para Blackboard y Moodle

¿Otras?

Gracias por la atención