CONVOCATORIA DE PREMIOS @ASLAN
A PROYECTOS DE TRANSFORMACIÓN DIGITAL EN ADMINISTRACIONES Y ORGANISMOS PÚBLICOS

SEGURIDAD COLABORATIVA: INCORPORACIÓN DEL USUARIO AL ECOSISTEMA DE SEGURIDAD EN MINETAD

Implantado en: MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

ANTECEDENTES/PROBLEMÁTICA

El Ministerio de Energía, Turismo y Agenda Digital (MINETAD) es pionero en la adopción de las medidas de seguridad requeridas por el **Esquema Nacional de Seguridad** (Real Decreto 3/2010, de 8 de enero), tendente a establecer unas condiciones de confianza en las relaciones por medios electrónicos entre los ciudadanos y las Administraciones Públicas, y se haya plenamente alineado con uno de los principales objetivos de la **Agenda Digital para España** centrado en "Reforzar la confianza en el ámbito digital" y desarrollado a través del **Plan de Confianza Digital**.

La Subdirección General de Tecnologías de la Información y de las Comunicaciones (SGTIC) del Ministerio, que es la encargada de desarrollar, operar y mantener la red informática corporativa y sus servicios asociados, es consciente de la importancia de llevar a cabo una securización de los elementos que la componen en base al nivel de seguridad que le es legalmente exigible.

La seguridad, entendida como un proceso integral y transversal a todo el Ministerio, conforma un ecosistema que abarca procedimientos, tecnologías y personas en el que, tradicionalmente, las

organizaciones han concentrado el grueso de sus inversiones y esfuerzos en las tecnologías y, en menor medida, los procedimientos, quedando el componente humano relegado a segundo plano.

Sin embargo, es un hecho constatado que las personas son el elemento más débil de la cadena de seguridad y, por tanto, el principal objetivo de las amenazas informáticas, además de ser la principal fuente generadora de problemas derivados de una mala compresión del uso de las tecnologías, por lo que la tendencia actual es considerar el elemento humano como uno de los principales activos de la organización y, en particular, un elemento imprescindible en la protección activa frente amenazas.

Es por ello que la SGTIC ha realizado un gran esfuerzo por incorporar a sus usuarios en el ecosistema de seguridad del Ministerio. Dado que la mayoría de los ataques detectados, y que no fueron cubiertos por la seguridad perimetral de los sistemas, usaron como vector de entrada el correo electrónico a usuarios (ataques de phising y distribución de enlaces maliciosos), se propuso en enero de 2016 un método basado en la concienciación en materia de seguridad de la información entre sus empleados que, junto con el resto de medidas técnicas previamente implantadas por la SGTIC, mitigase el impacto de dichas amenazas, con los siguientes ejes de actuación:

- Eje organizativo: con segmentación de perfiles y personalización de mensajes y actuaciones según exposición al riesgo de los colectivos y descubrimiento de casos de infección.

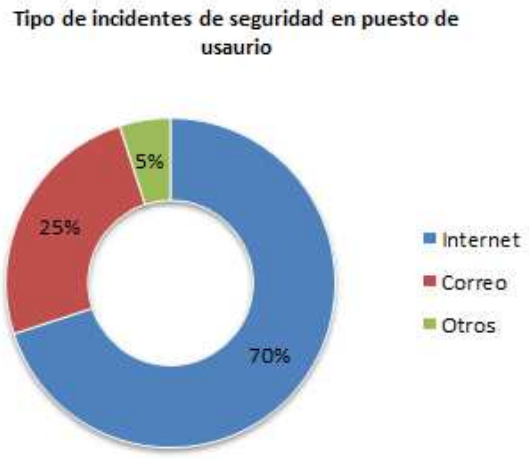
- Eje tecnológico: con una solución técnica que permite diseñar campañas de comunicación dirigidas a partir de un repositorio de contenidos de relevancia en materia de seguridad de la información, y que se distribuyen al puesto de trabajo de los usuarios internos del Ministerio. Los formatos de comunicación y medios de transmisión pueden seleccionarse según distintos criterios y en función del perfil de los usuarios.

- Eje de mejora continua: a partir de cuadros de mando de indicadores de lectura y eficiencia de la comunicación y medición de la respuesta por parte de los usuarios ante nuevos ataques.

Durante el año se han realizado varias campañas de comunicación y concienciación, mejorando así la resiliencia del sistema y promoviendo la colaboración activa de todos los usuarios de la red del MINETAD.

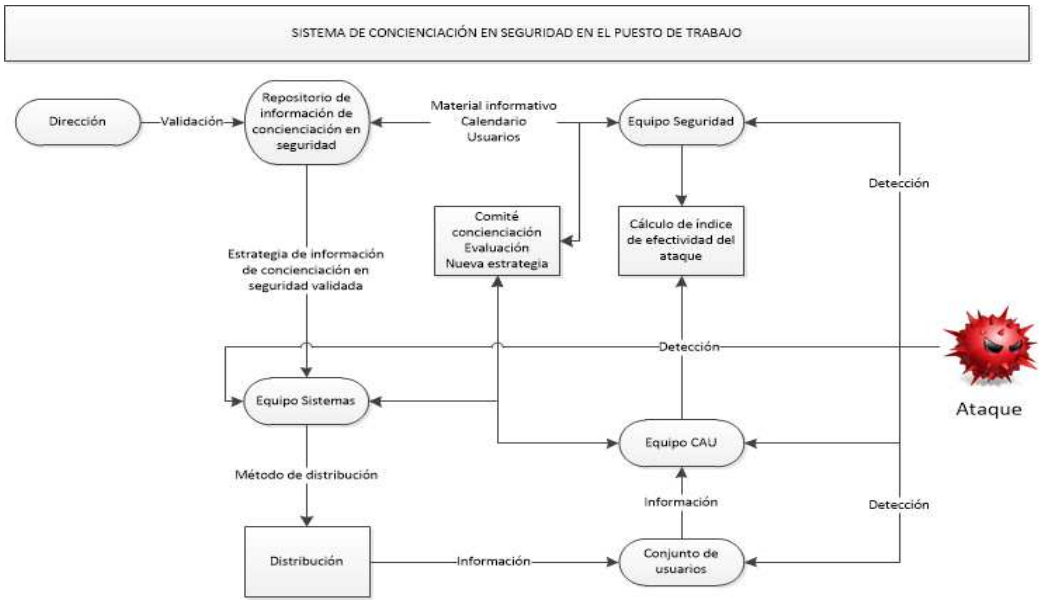
OBJETIVOS PERSEGUIDOS

Si se analiza la siguiente figura se observa que, de las alertas de seguridad reportadas por los distintos elementos de seguridad desplegados en el MINETAD, un 20% del total se corresponden a eventos directamente relacionados con la actividad del usuario. De esa cifra, la mayoría de las alertas se materializan en un incidente de seguridad en el puesto de usuario, cuya causa directa se debe a malos hábitos de navegación por internet, ataques de phising y correos con elementos maliciosos en su contenido y/o anexos.



El principal objetivo consistió en dotar a los empleados del Ministerio de una "**cultura de la ciberseguridad**" mediante la difusión entre los mismos de la normativa y procedimientos internos en materia de seguridad de la información, en informarles y concienciarles sobre el uso seguro de la navegación web, y en minimizar el impacto de los ataques de phising recibidos por correo electrónico gracias al reconocimiento activo por parte del usuario de ese tipo de mensaje que, por una parte le hiciera ignorar su contenido e instrucciones **(seguridad reactiva)** y, por otra parte, le instase a informar al Centro de Atención a Usuarios (CAU) ante cualquier correo sospechoso (**seguridad preventiva**).

Para ello fue necesario crear un repositorio que aglutinase la información e instrucciones a distribuir, habilitar los canales de distribución y planificar las campañas de concienciación y, por último, establecer unos mecanismos de medición del grado de éxito de las mismas, a fin de reprogramar nuevas difusiones o focalizar en ciertos grupos de usuarios menos concienciados, tal y como se describe en la siguiente figura:



FASES DEL PROYECTO – RECURSOS EMPLEADOS

En proyecto se inició en enero de 2016 y desde esa fecha se han realizado distintas **campañas de concienciación** orientadas a difundir la normativa de seguridad de la información, las buenas prácticas para una navegación segura por internet, al reconocimiento de correos fraudulentos (phising) o recepción de adjuntos maliciosos que hayan podido pasar desapercibidos para los sistemas perimetrales de detección de amenazas, y el envío periódico de mensajes preventivos frente a campañas malware específicas (ej. "factura de ENDESA", "devolución AEAT pendiente" y "entrega de paquete de Correos").

La herramienta habitual para la difusión de las campañas de concienciación ha sido el envío secuencial de correos personalizados a los usuarios, que además se ha visto complementado con publicaciones periódicas en la intranet de recomendaciones en materia de seguridad de la información, y se ha contado también con el apoyo de otros medios tecnológicos como son salvapantallas y fondos de escritorio personalizados por la SGTIC con los mensajes que se querían difundir, desplegados de forma centralizada mediante políticas GPO, mensajes tipo POP a colecciones de máquinas aleatorias con SCCM, mensajes de inicio de sesión y ventanas con mensajes emergentes.

La elaboración y difusión de las campañas de concienciación han pasado a formar parte de la operativa estándar de la SGTIC, e involucra a numerosos recursos del MINETAD, tanto personal propio como de asistencia, como son la alta dirección, el equipo de seguridad informática, diseñadores de contenidos, administradores de correo, administradores de directorio activo, y personal de apoyo al usuario.

El contenido utilizado en las campañas de concienciación ha sido de elaboración propia y siguiendo las recomendaciones proporcionadas por el Centro Criptológico Nacional, INCIBE y otros foros reconocidos en materia de ciberseguridad.

La ejecución de una campaña de concienciación típica consta de la siguiente estructura:

Selección de mensaje: Contenido que se quiere difundir.
Selección de canal: Campaña informativa por correo electrónico.
Remitente: Unidad Informática MINETAD.
Receptores: Todos los usuarios de la organización.
Duración: 4 semanas.
Formato: Mensaje electrónico en forma de imagen (ver anexo).
Periocidad: 1 mensaje semanal.
Contenido: Los 4 mensajes abordaran de forma secuencial esta temática:

- Semana 1: Enlaces recibidos por correo electrónico.
- Semana 2: Adjuntos recibidos por correo electrónico.
- Semana 3: Ofertas recibidas por correo electrónico.
- Semana 4: Formularios recibidos por correo electrónico.

Evaluación de la campaña: Comparativa con el número de incidentes mensuales cuyo origen haya sido el correo electrónico entregado a usuarios respecto del número obtenido al mes de finalizar la campaña.

Retroalimentación: En función de la evaluación se tomarán estas acciones:

- Reiteración a todos los usuarios con alteración de contenido y/o formato.
- Campañas específicas a colectivo de usuarios diferenciado.

A continuación, se muestra un ejemplo del tipo de contenido que se ha difundido en una campaña de concienciación usando el canal del correo electrónico:

MEJORAS EN EFICIENCIA Y REDUCCIONES DE COSTE

Las distintas campañas llevadas a cabo han servido para prevenir la materialización de distintos ataques que, de haber tenido éxito, hubieran supuesto la movilización de numerosos recursos del Ministerio, tanto para revertir la situación material (sustitución de equipos, recuperación de cuentas y buzones), como para mitigar la pérdida de reputación y confianza en el Ministerio asociados a una exfiltración de datos y/o robo de identidad.

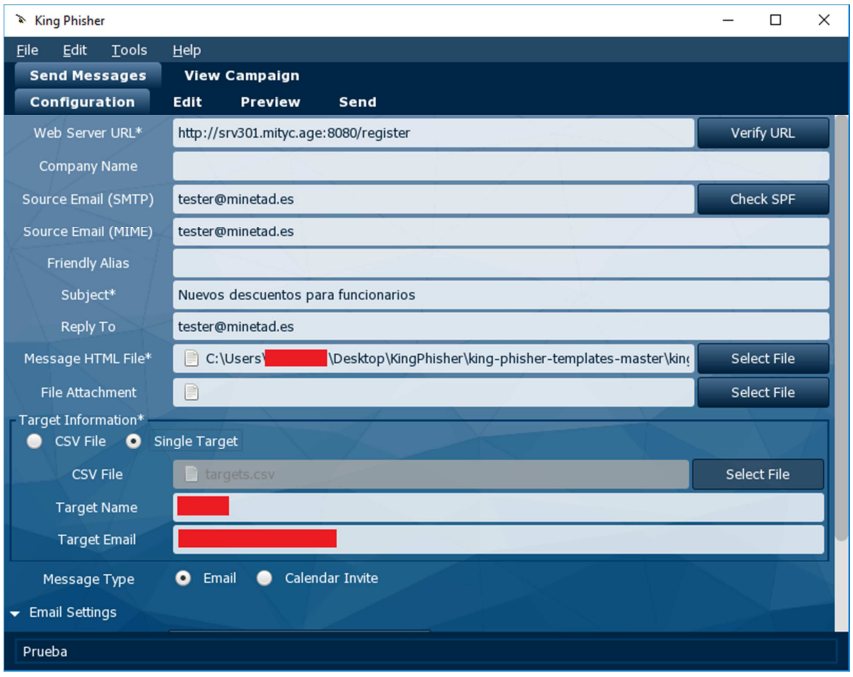
Se ha detectado una mayor proactividad por parte de usuarios con indicios de ataques o infecciones. Esta mayor colaboración de los usuarios ha permitido la actuación temprana por parte del equipo informático ante patrones muy difíciles de identificar.

Ante ataques reales, se ha comprobado una disminución del número de activos afectados, así como un aumento en la comunicación de estos incidentes al equipo de seguridad y se ha obtenido una mayor precisión en la categorización de los incidentes y, por tanto, una mayor eficiencia en la dedicación de recursos a casos de mayor criticidad.

La SGTIC dispone de la posibilidad de utilizar métricas para evaluar la eficiencia de las campañas de concienciación. Una de esas métricas es el **índice de penetración**, mediante el cual tenemos en cuenta el número de buzones de usuario que han sido objeto de una determinada campaña malware y podemos determinar cuántos de ellos han seguido las instrucciones del correo malicioso frente a

cuentos han hecho caso omiso o bien han reportado el incidente, y comparar estos datos con otras campañas malware previas a la concienciación.

Para poder utilizar métricas de forma precisa, el equipo de seguridad de la SGTIC ha creado un entorno controlado para distribuir de forma interna campañas de correo malware de prueba y medir la eficacia de las medidas de concienciación a ajustar el target de las campañas al tipo de usuario.



CONCLUSIONES DE LA ENTIDAD

La puesta en marcha de las distintas campañas de concienciación ha permitido que el usuario sea consciente de que **la seguridad de la información en la organización es asunto de todos** y que este se haya convertido en parte esencial del ecosistema de seguridad del Ministerio.

Por una parte, las acciones de los empleados en el uso diario de herramientas de comunicación tienen ahora un componente en el que el usuario sabe valorar el riesgo asociado a ellas y, por otra parte, el usuario se ha convertido en fuente generadora de alertas sobre posibles eventos de seguridad al estar capacitado para reconocer cierto tipo de ataques que antes le pasaban desapercibidos.

La concienciación en materia de seguridad dirigida a los empleados, tal y como establecen las principales guías y estándares, y así se recoge en la **Política de Seguridad de la Información** del Ministerio, ha pasado a ser una línea de acción fundamental que cuenta con el total apoyo de la alta dirección (**Comité de Seguridad de la Información**).

La inversión de recursos y medios, tanto materiales como humanos, realizada por el Ministerio en materia de concienciación se ha convertido en una línea de acción continuista en el tiempo a ejecutar por la SGTIC debido al contrastado retorno de la inversión, que no solo asegura la resiliencia de la organización frente a las amenazas externas, sino que minimiza los costes asociados, tanto monetarios como reputacionales, que se derivarían de la materialización de los ataques.