tracasa instrumental

18.01.2024

Una plantilla entrenada en ciberseguridad para cambiar nuestro comportamiento

Índice

1 Tracasa Instrumental

Tracasa Instrumental es una sociedad pública del Gobierno de Navarra adscrita al departamento de Universidad, Innovación y Transformación Digital.

Gobierno de Navarra
Nafarroako Gobernua

Es el ente instrumental de referencia para el Gobierno de Navarra en servicios y conocimientos de transformación digital, gestión tributaria, gestión del territorio y atención a la ciudadanía. La vocación de mejora continua, la calidad, la innovación y el desarrollo profesional de nuestros equipos son aspectos prioritarios para desarrollar y sostener el valor en nuestros servicios para el Gobierno y la sociedad.

Tracasa Instrumental

tracasa instrumental

Tracasa Instrumental, sociedad pública del Gobierno de Navarra, es la empresa de referencia para el Ejecutivo Foral en servicios y conocimientos de transformación digital, gestión tributaria, gestión del territorio y atención a la ciudadanía.

Nuestra misión principal es apoyar al Gobierno de Navarra para que sea más eficiente y seguro en sus actuaciones, contribuyendo a ofrecer el mejor servicio posible a la sociedad navarra.

Tracasa Instrumental aporta valor tecnológico, innovación y alto desempeño en servicios que son estratégicos para el Gobierno de Navarra como Salud, Justicia, Hacienda, Catastro, Policías y Emergencias, Administración Electrónica, Educación e Información del Territorio.

600	41	28M	03
Profesionales	Años de experiencia	Cifra de negocio	Áreas de negocio

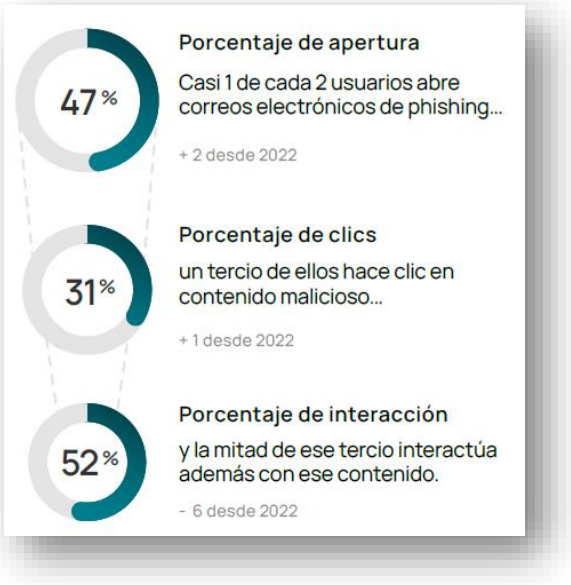
Datos 2023

2 Antecedentes

2.1 Contexto general de análisis de riesgo humano

La tensión mundial, los conflictos geopolíticos y las constantes interrupciones de la actividad empresarial han creado un mundo volátil, lo que aumenta drásticamente la superficie de ataque de los ciberdelincuentes y los lleva a profesionalizar aún más sus modelos de negocio. Al mismo tiempo, avances tecnológicos como las herramientas de IA generativa han democratizado el «arte de la ciberdelincuencia». El resultado es que hoy en día nos hallamos frente a innumerables hackers potenciales que disponen de las herramientas necesarias no solo para maximizar el alcance de sus ataques, sino también su porcentaje de éxito. Llevamos un tiempo observando que los ciberdelincuentes podrían utilizar tácticas sofisticadas basadas en la IA, como los

deepfakes, para perpetrar ataques a gran escala. Recientemente se ha facilitado el acceso a herramientas muy potentes de IA generativa, poniendo la ciberdelincuencia al alcance de cualquiera. Como resultado de todo ello, recientes estudios recogen estadísticas como las siguientes:



Por definición, la ciberseguridad debe evolucionar y adaptarse constantemente, y también forma parte de ella adoptar nuevas tecnologías para mantenernos mejor protegidos frente a las nuevas tácticas de ataque. Pero si de algo podemos estar seguros es de que los atacantes seguirán intentando encontrar la manera de sortear incluso las barreras tecnológicas más sofisticadas; y a menudo lo conseguirán.

En los últimos años se ha visto un cambio en la estrategia de ataque de los ciberdelincuentes. Ya no se trata de atacar a los sistemas, de intentar burlar las barreras que tenemos, sino de atacar a las personas que utilizan dichos sistemas. Los hackers utilizan ingeniería social para analizar a las personas, buscan cuáles son más vulnerables dentro de una organización y qué hábitos tienen. Utilizan técnicas como meter prisa ("esto o lo hacemos ahora o perdemos el negocio"), la discreción ("no lo comentes que este tema quiero que lo llevemos entre tú y yo"), y se aprovechan del respeto o incluso miedo a algunas figuras de autoridad.

Son plenamente conscientes de que su máxima garantía de éxito es jugar con las emociones de las personas, y así lo vienen demostrando con los últimos ataques de phishing que hemos conocido por ser los más mediáticos.

Por este motivo, no es de extrañar que la sensibilización encabece la lista de prioridades en materia de seguridad entre la mayoría de organizaciones tanto del sector público al que pertenecemos como del sector privado, y Tracasa Instrumental no es una excepción a este escenario.

2.2 Situación de partida de Tracasa Instrumental

Tracasa Instrumental es una organización que, en el ámbito de su seguridad digital, ha desarrollado desde hace más de 10 años un Sistema de Gestión de la Seguridad de la Información (SGSI) certificado bajo el estándar internacional ISO 27000 y adaptado tanto al Esquema Nacional de Seguridad (ENS) como al Reglamento General de Protección de Datos (RGPD).

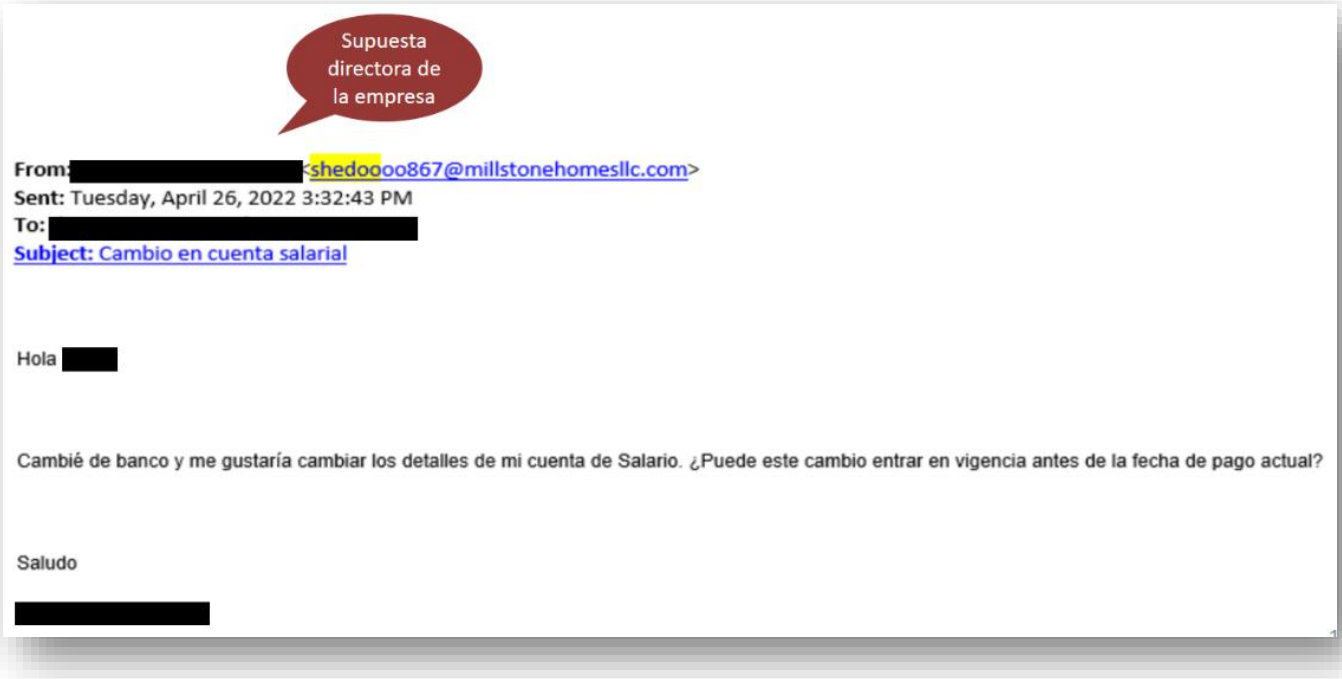
En lo referente a la concienciación y capacitación de la plantilla, en su planificación anual establecía una serie de acciones de formación y concienciación en ciberseguridad, así como una sesión dentro del plan de acogida a las nuevas incorporaciones. También se reforzaba con comunicaciones corporativas periódicas, en las que se advertía de nuevos riesgos potenciales y se ilustraban buenas prácticas de seguridad digital.

Este planteamiento adolecía, no obstante, de una sistemática programada y personalizada a los distintos perfiles y posicionamiento respecto al riesgo de la plantilla, sin un contenido previamente elaborado y que fuera automáticamente actualizado con novedades en materia de ciberseguridad.
En lo referente a ingeniería social, no había campañas de simulación de phishing.

La compañía realizó un ejercicio de hacking ético (Red Team) en el que se evidenciaron las carencias de algunos empleados en la identificación de acciones de ingeniería social.

2.3 Intento de phishing a punto de ser exitoso

En el mes de abril de 2022 la compañía sufrió un intento de phishing que, a pesar de ser muy poco sofisticado, estuvo a punto de ser exitoso.



Partiendo del diagnóstico anteriormente descrito, este hecho fue el detonante que impulsó al área de Seguridad Digital a lanzar este proyecto de entrenamiento de ciberseguridad que proporcionara a la organización un enfoque de solución distinto al empleado hasta el momento.

Está comprobado que la formación en ciberseguridad requiere de metodologías de aprendizaje diferentes a las tradicionales para adquirir, de forma más eficiente, las competencias esenciales necesarias.

3 Descripción del proyecto

3.1 Estrategia del proyecto

Tracasa Instrumental estableció como objetivo del proyecto un cambio en el comportamiento de los usuarios, es decir, se trataba de un proyecto de cambio cultural organizacional y no de un proyecto tecnológico.

Para ello, el Plan Director 2020-2023 actuó como palanca de cambio en cuanto a que establecía objetivos y acciones específicas en el ámbito de la ciberseguridad que facilitaban la gestión del cambio. De esta forma, la Dirección General y las direcciones de los departamentos actuaron como agentes impulsores del proyecto.

Así mismo, esta iniciativa debía encajar con el marco de trabajo de mejora continua de la organización, en lo referente a la medición inicial, el desarrollo de las acciones, la valoración de la eficacia de dichas acciones y la identificación de puntos de mejora que desencadenen nuevas acciones.

Partiendo de todo ello, Tracasa Instrumental estableció las siguientes fases de proyecto:

- Evaluación inicial: determinando la base de referencia de Tracasa Instrumental y los riesgos en cuanto a concienciación en seguridad. Identificación de las carencias de conocimientos de los usuarios y cuáles son sus actitudes y opiniones sobre la seguridad, para poder determinar mejor la formación para concienciación en materia de seguridad que necesitan, y asignando las simulaciones y evaluaciones adecuadas.
- Cambio del comportamiento de los usuarios: estimulando la participación y proporcionando formación en ciberseguridad dirigida y personalizable según su función, competencias, vulnerabilidades y estilo de aprendizaje.
- Evaluación: evaluando el resultado del programa, midiendo e informando del progreso tanto al usuario como a los responsables a lo largo del tiempo, mediante indicadores que capten cómo cambian los comportamientos, vulnerabilidades de los usuarios y análisis comparativos con empresas similares del sector.

Para ello se debían implementar, al menos, estas dos funcionalidades principales:

- Módulos de aprendizaje: los contenidos debían ser iterativos, amigables y de corta duración. El itinerario formativo debía poder ser configurable y personalizable por perfiles, áreas, colectivos, desempeño en el programa, etc.
- Campañas de simulación de phishing: configurables y administrables por Tracasa Instrumental.

El alcance del proyecto debía ser global, es decir, abarcando la totalidad de la plantilla y del personal externo que se integra en los procesos de trabajo de Tracasa Instrumental, por lo que el número de usuarios ascendió a entorno 700.

La estrategia de arranque debía ser en modo “big bang”: un único arranque con toda la funcionalidad, todas las localizaciones y todas las unidades de negocio, ya que los riesgos están extendidos al conjunto de la organización.

3.2 Motor de cambio para otras organizaciones: 18 sociedades públicas navarras

Tracasa Instrumental, al igual que el resto de sociedades públicas, pertenece a la Corporación Pública Empresarial de Navarra (CPEN). CPEN tiene como misión de ser el instrumento unitario de ordenación y racionalización de las sociedades públicas de Navarra, y está compuesta por las 18 empresas públicas de Navarra.

CPEN formó en 2021 un Grupo de Trabajo de Ciberseguridad coordinado por Tracasa Instrumental cuyo objetivo es mejorar el estado de la ciberseguridad del conjunto de las 18 sociedades, la mayoría de ellas con menor perfil tecnológico.

En este contexto, este proyecto de Tracasa Instrumental se enfocó estratégicamente como la primera experiencia de la CPEN en entrenamiento en ciberseguridad que permitiera, en el caso de ser exitosa, extenderse al total de las sociedades actuando así de palanca de cambio.

La satisfacción resultante con el proyecto de Tracasa Instrumental permitió que en septiembre de 2023 CPEN lanzara este proyecto para el resto de las 17 sociedades públicas de Navarra.

Actualmente, por lo tanto, el conjunto de las 18 sociedades públicas y la totalidad de la plantilla de más de 1.600 profesionales está trabajando con este programa de entrenamiento de ciberseguridad.

3.3 Alcance funcional

3.3.1 Uso de una plataforma especializada

Para poder abarcar los objetivos del proyecto se consideró necesario la utilización de una plataforma especializada en entrenamiento en ciberseguridad. Este tipo de plataformas permiten realizar la gestión de programas de entrenamiento de una forma integral, aunando en un mismo sitio tanto el envío del contenido formativo y de las simulaciones de ataque como la información relativa al desempeño en ambos.

La plataforma seleccionada fue Proofpoint Security Awareness Training (PSAT), de la compañía Proofpoint.

A continuación, se describen las funcionalidades de la plataforma que se están utilizando en el programa de entrenamiento desarrollado:

3.3.1.1 Módulos de aprendizaje

Se incluyen conocimientos conceptuales de forma práctica, para aprender más fácilmente las acciones necesarias para identificar o resolver un problema.

- El conocimiento está adaptado a las situaciones reales de las personas usuarias. De esta forma, se recuerda mejor el contexto que el contenido en sí.
- El contenido se ofrece en pequeñas dosis, porque las sesiones cortas de entrenamiento son más eficaces.
- El mismo conocimiento se transmite de diferentes formas, ya que, al presentar un mismo concepto con enunciados y términos diferentes, es más fácil asociarlos a experiencias pasadas y establecer nuevas conexiones.
- En cada módulo se incluye una evaluación inmediata para fijar el aprendizaje, y lo aprendido se refuerza con ejercicios prácticos y ataques simulados.
- Cada persona puede marcar su ritmo, aunque se recomienda seguir las asignaciones programadas para un mejor aprovechamiento del curso.

La elaboración del itinerario formativo es un elemento crucial, tanto por el contenido en sí mismo, buscando que sea útil y atractivo, como por el equilibrio necesario entre la cantidad de contenidos y la dedicación de tiempo que han de tener los usuarios para completarlos, evitando así que se pierda la motivación.
La personalización del contenido de algunos módulos, en especial aquellos relacionados con las políticas de seguridad de la información de Tracasa Instrumental, es un elemento importante que acerca el contenido a la realidad de los usuarios, que lo perciben como algo más cercano, lo cual redunda en un mayor aprovechamiento del mismo.

3.3.1.2 Simulaciones de phishing

La inteligencia de amenazas que incorpora la herramienta alimenta nuestras simulaciones de phishing con amenazas reales obtenidas en entornos de producción. Esta inteligencia de amenazas tiene acceso a información de millones de correos enviados cada día.
Se dispone de los derechos de uso de logos y marcas conocidas (Google, Whatsapp, Owncloud, etc.) para recrear escenarios de phishing muy reales.

También disponemos de la capacidad de crear nosotros mismos las campañas que phishing que consideremos, de forma muy sencilla y sin requerir de conocimientos técnicos.
Todas estas opciones nos facilitan muchas alternativas a la hora de personalizar las campañas, ya que podemos determinar la complejidad de las mismas, así como su frecuencia, colectivos a los que se dirige, etc. Por otro lado, nos permite adaptar los ejercicios de simulación a las amenazas reales que se concentran alrededor de algún evento concreto, como por ejemplo las compras de Black Friday o la campaña de la declaración de la renta. Mediante la combinación de diferentes tipos de simulación y niveles de dificultad podremos detectar vulnerabilidades en nuestros usuarios.

3.3.1.3 Cuestionarios de evaluación
El envío de cuestionarios de evaluación proporciona una valoración del conocimiento en ciberseguridad de la organización. La realización de los mismos en diferentes momentos del desarrollo del programa nos permite analizar el grado de mejora en el conocimiento de los usuarios en la materia, siendo a la vez un elemento que fomenta la participación en el programa.

3.3.1.4 Reporte del phishing
La herramienta se integra con el servicio de correo proporcionando un botón donde los usuarios podrán reportar posibles amenazas de correos de phishing. Si el correo reportado es fruto de una simulación, el sistema lo detecta y lo añade a la información proporcionada por la plataforma. Este dato es muy importante como indicador de cuánto están contribuyendo los usuarios a la defensa contra las amenazas.

3.3.1.5 Comunicaciones desde la plataforma
La interacción con los usuarios se realiza mediante notificaciones a través del correo electrónico, donde se informa de los nuevos contenidos puestos a disposición del personal de Tracasa Instrumental para su formación. Además, el sistema permite configurar notificaciones automáticas de recordatorio, que se envían periódicamente a las personas que tienen contenidos pendientes. Esto ayuda a aumentar la participación en el programa, ya que el acceso es sencillo y se reduce al mínimo la posibilidad de perder el acceso.
Por otro lado, el acceso se sincroniza con el sistema de Single Sign On de la empresa, con lo cual se evita la gestión de accesos y contraseñas.

3.3.1.6 Informes
Se dispone en tiempo real de toda la información necesaria para realizar el seguimiento del programa, y que dará la posibilidad de reaccionar con agilidad a las diferentes situaciones que se pueden dar. A modo de ejemplo, se enumeran a continuación la información que más está utilizando Tracasa Instrumental:

- Participación: mediante la información de los módulos realizados por cada usuario, así como la puntuación obtenida en las evaluaciones finales de cada módulo.
- Desempeño en simulaciones: mediante datos de caídas en simulaciones, podemos detectar a los usuarios más vulnerables, o que necesitan algún tipo de refuerzo en su formación.
- Resultado de los cuestionarios: para evaluar la evolución de la base de conocimiento de la organización.
- Comparativa entre campañas de simulación: nos permitirá modular la dificultad de las campañas, en función de los objetivos buscados en cada momento.
- Benchmarking: resultados de nuestra empresa en comparación con empresas equivalentes del sector.

3.3.2 El reto: conseguir una alta participación

Durante la primera versión del programa, el reto para Tracasa Instrumental era conseguir una alta participación del conjunto de la plantilla, así como del personal externo integrado en nuestros procesos de trabajo. De esta forma, el objetivo era enraizar el programa en el día a día del trabajador, de forma que se fuera instalando una sólida cultura de la ciberseguridad.
Así mismo, la empresa ha experimentado un fuerte incremento de plantilla en los últimos años por lo que un aspecto fundamental del proyecto era impregnar a los nuevos trabajadores de esa cultura y sensibilización por la ciberseguridad.

Afortunadamente el objetivo de participación fue alcanzado plenamente, superando el 80% y bastante por encima de la media de los indicadores de benchmarking que la propia herramienta facilita y obtiene de toda la base de datos de sus clientes.

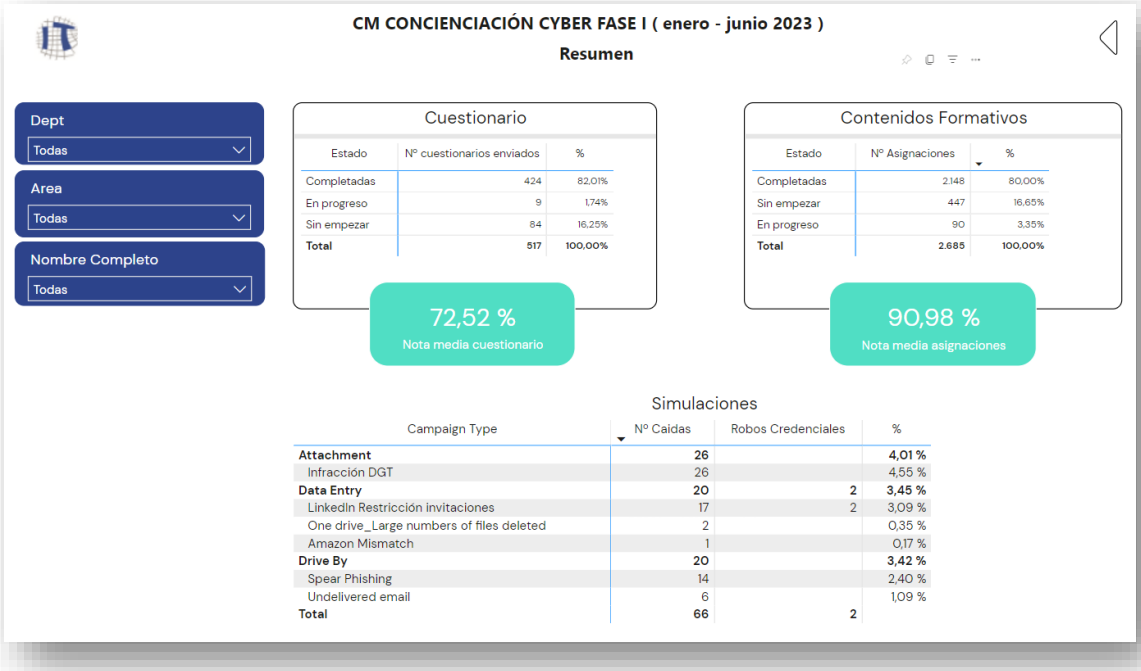
Consideramos que las principales claves para haber conseguido el objetivo fueron las siguientes:

1. Impulso de la Dirección y de los mandos intermedios, que asumió el proyecto como propio y actuó como palanca de cambio para toda la organización.
2. Selección de una plataforma solvente, siendo en el momento de la contratación la única solución homologada por el Centro Criptológico Nacional (CCN) dentro de su Catálogo de Productos y Servicios STIC.
3. Usabilidad de la herramienta, ya que resulta muy cómoda de utilizar, integrada mediante SSO con nuestro Directorio Activo de Azure y los contenidos y formatos son muy amigables.
4. Contenidos de ciberseguridad útiles también para la vida personal del empleado y de su familia, lo que hace que el trabajador adquiera un mayor interés en el programa.
5. Equilibrio en el volumen de contenidos, puesto que se estableció un número de minutos que dotara de contenido al programa pero que no supusiera una excesiva dedicación en el día a día del empleado. El tiempo medido de dedicación se estableció en 1 hora al mes aproximadamente.
6. Partner integrador de total confianza, gran conocedor de la plataforma y prestando un servicio excelente en todas las fases del proyecto (diseño, ejecución y soporte).
7. Desarrollo propio de Cuadros de Mando, que permitieron a los mandos intermedios realizar un seguimiento de cumplimiento de los equipos de forma muy sencilla.
8. Apoyo del área de Comunicación, diseñando las campañas de comunicación interna adecuadas para conseguir el compromiso de toda la organización.

3.3.3 Otros resultados obtenidos

Se han obtenido otros resultados positivos de indicadores, como una tasa de caídas en phishing del 1,8% (promedio del sector en el 12%) o un reporte de correos electrónicos correctamente reportados como phishing del 37,9% (promedio del sector del 13%).

A modo de referencia, se adjunta el resumen de indicadores de la versión 1 del programa:



CM CONCIENCIACIÓN CYBER FASE I (enero - junio 2023)

Resumen

Dept: Todas

Area: Todas

Nombre Completo: Todas

Cuestionario

Estado	Nº cuestionarios enviados	%
Completadas	424	82,01%
En progreso	9	1,74%
Sin empezar	84	16,25%
Total	**517**	**100,00%**

72,52 %
Nota media cuestionario

Contenidos Formativos

Estado	Nº Asignaciones	%
Completadas	2.148	80,00%
Sin empezar	447	16,65%
En progreso	90	3,35%
Total	**2.685**	**100,00%**

90,98 %
Nota media asignaciones

Simulaciones

Campaign Type	Nº Caidas	Robos Credenciales	%
Attachment	**26**		**4,01 %**
Infracción DGT	26		4,55 %
Data Entry	**20**	**2**	**3,45 %**
LinkedIn Restricción invitaciones	17	2	3,09 %
One drive_Large numbers of files deleted	2		0,35 %
Amazon Mismatch	1		0,17 %
Drive By	**20**		**3,42 %**
Spear Phishing	14		2,40 %
Undelivered email	6		1,09 %
Total	**66**	**2**	

3.3.4 Detección de un phishing sofisticado

En septiembre de 2023, el área de la empresa que recibió el phishing en abril de 2022 y que estuvo a punto de caer en el mismo, recibió un intento de phishing mucho más sofisticado que el anterior. Los empleados del área identificaron el correo electrónico como phishing y lo reportaron.

Este hecho, que puede catalogarse como anecdótico, supuso para el equipo de proyecto una gran satisfacción ya que evidenció que el programa estaba resultando eficaz.

3.3.5 El programa, una apuesta de futuro

Después de casi un año de uso, Tracasa Instrumental ha consolidado ya este programa y lo tiene integrado en sus procedimientos y en el día a día de sus trabajadores.

Si pensamos en la evolución habitual de un proyecto de estas características desde el punto de vista del progreso en el comportamiento de los usuarios de una organización, estas suelen ser las prioridades:

• Versión 1: Participación. Adquirir consciencia de las amenazas y de los comportamientos adecuados por parte de los usuarios.
• Versión 2: Resultados ante las amenazas. Saber comportarse con solvencia identificando y gestionando amenazas de mayores niveles de dificultad.
• Versión 3: Resiliencia. Informar de las amenazas al administrador, afianzando un factor de resiliencia destacado como organización.

En la ejecución de la versión 1 del programa se elaboró un itinerario preliminar o de inmersión, que se ejecutó de forma conjunta en toda la empresa. De esta forma, se aseguró el aprendizaje de conceptos básicos y un lenguaje común para todos los usuarios, a la vez que nos permitió tener datos de cumplimiento con criterios comunes y así poder hacer más adelante una diferenciación en función de algunos parámetros.

Actualmente Tracasa Instrumental se encuentra inmersa en la versión 2 del programa, centrando los esfuerzos en mantener o mejorar la participación, así como gestionar determinados colectivos principalmente aquellos que caen en las campañas de phishing y no cumplimentan los módulos de ciberseguridad. Para ello se están ejecutando dos itinerarios:

- Un itinerario de desarrollo para las personas que tuvieron un buen desempeño en la versión 1 del programa, con menor carga formativa, pero que incluye la asignación de contenidos de refuerzo a los usuarios que caigan en una simulación de ataque. Con este itinerario se pretende consolidar los conocimientos adquiridos y fortalecer la capacidad de reacción ante las amenazas modulando el contenido entregado en función del desempeño con las simulaciones.
- Un itinerario esencial para las personas que se han incorporado recientemente a la organización, que a la vez sirve de repesca para los usuarios "rezagados" de la versión 1.

Tracasa Instrumental entiende la cultura de la ciberseguridad en la organización como un proceso continuo, en el que además deben incorporarse todas las novedades de ciberamenazas que el entorno presenta, y por lo tanto este programa en un futuro dejará de ser un proyecto para ser un servicio continuo corporativo.

4 Repercusión para la ciudadanía y las administraciones

Tracasa Instrumental es la principal empresa tecnológica del Gobierno de Navarra y la primera empresa pública de la Administración Foral de Navarra, con cerca de 700 empleados que representan más del 40% de la masa de trabajadores del sector público en la Comunidad Foral.

Como hemos descrito en el primer apartado, Tracasa Instrumental es la empresa de referencia para el Gobierno de Navarra en servicios y conocimientos de transformación digital, gestión tributaria, gestión del territorio y atención a la ciudadanía, contribuyendo de manera significativa a la modernización de la sociedad navarra.

Tracasa Instrumental aporta valor tecnológico, innovación y alto desempeño en servicios que son estratégicos para el Gobierno de Navarra como Salud, Justicia, Hacienda, Catastro, Policías y Emergencias, Administración Electrónica, Educación e Información del Territorio.
En este contexto, disponer de trabajadores entrenados en ciberseguridad minimizando así el riesgo de sufrir un ciberataque al ser este el principal vector de ataque en la actualidad, y que puedan servir de ejemplo para otras organizaciones con las que trabajamos, quizás más lejanas a la tecnología, proporciona un impacto sin duda alguna muy positivo en la ciudadanía y en el conjunto de administraciones públicas con las que interactuamos y nos integramos.

5 Equipo de desarrollo y proveedores

El equipo de proyecto ha estado compuesto principalmente por los siguientes roles:

- Dirección de la empresa
- Responsable de Seguridad de la Información
- Responsable IT
- Empresa Nextpand, como integrador de la solución
- Proofpoint, como fabricante del producto

6 Valoración económica

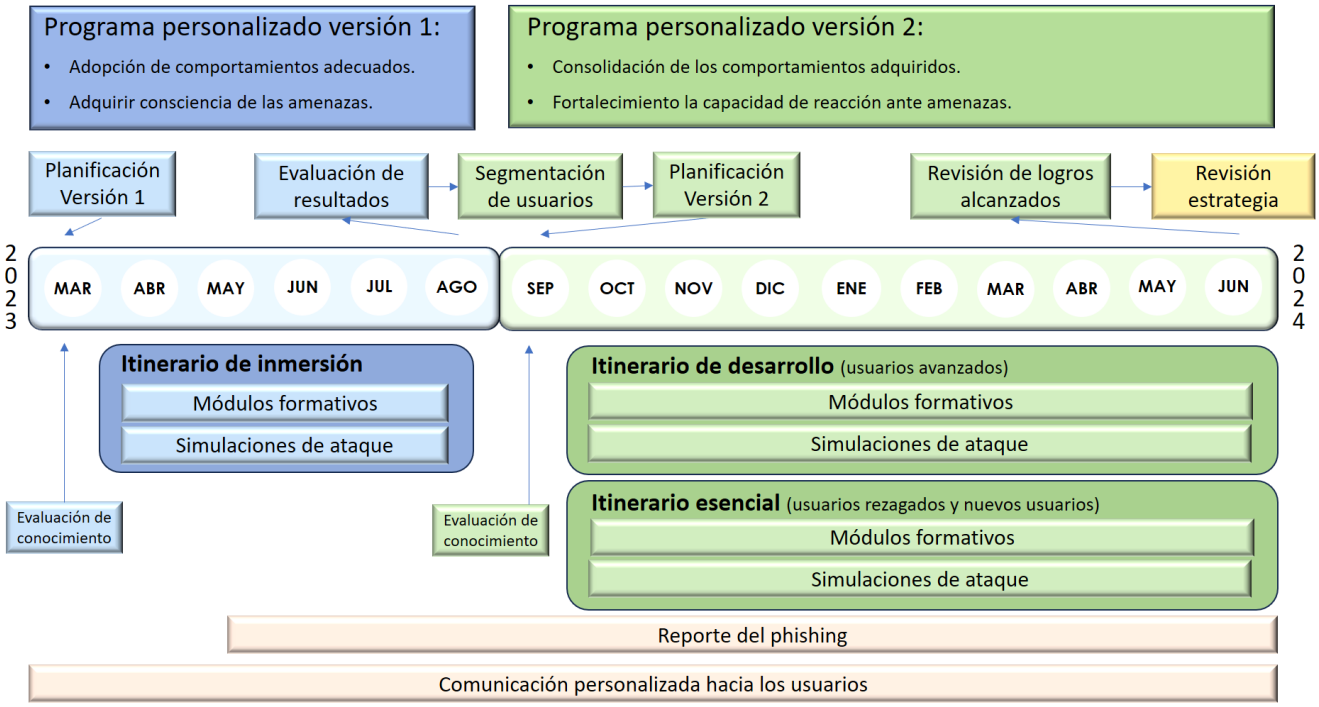
El proyecto ha tenido un presupuesto de 14.870 euros durante 12 meses, para los servicios de puesta en marcha de la plataforma de concienciación de seguridad y 700 suscripciones de producto anuales.

7 Plazos de cumplimiento

Previamente al proyecto de ejecución, hubo una fase interna de definición de requisitos, prospección de mercado de plataformas y partners y análisis de experiencias similares de éxito tanto en el sector público como privado. Esta fase tuvo una duración aproximada de 5 meses.

El proyecto de ejecución se inició en marzo de 2023 estableciéndose para la versión 1 una duración de 6 meses, finalizando por lo tanto en agosto de 2023.
La versión 2 se inició en septiembre de 2023 y finalizará en junio de 2024.

El detalle de cronograma de proyecto es el siguiente:



8 Lecciones aprendidas

Tracasa Instrumental emplea marcos ágiles de desarrollo en sus proyectos, y por lo tanto celebramos retrospectivas agile mediante las cuales los equipos reflexionan sobre qué salió bien y qué podría mejorarse. Las consideramos esenciales para mejorar continuamente el proceso y garantizar así que se incorporen los aprendizajes clave para las siguientes iteraciones o proyectos.

Las principales lecciones aprendidas de este proyecto han sido las siguientes:

- El aprendizaje y el entrenamiento de la ciberseguridad es un proceso complejo y muy cambiante, que requiere de aproximaciones metodológicas de aprendizaje distintas a las tradicionales.
- El liderazgo de la Dirección es fundamental para el éxito de este tipo de proyectos, horizontales y de cambio cultural. Sin su apoyo es muy difícil conseguir una alta participación.
  También se requiere el apoyo de Operaciones, en la medida en que vamos a destinar una parte del tiempo de los trabajadores a formarse y entrenarse.
- La implicación del equipo interno, la correcta elección de un partner especializado en programas personalizados y de una plataforma solvente son clave para el éxito del proyecto.
- La cultura de la ciberseguridad es una carrera de fondo, no te desanimes si los resultados iniciales no son los esperados. Lo más importante y lo más difícil es empezar el camino e ir sembrando la organización con concienciación y entrenamiento en seguridad digital.

8.1 Último tip

Si toda o parte de la Dirección no apoya suficientemente el proyecto, lánzales una campaña de simulación de phishing. Será la mejor evidencia de la necesidad del programa…

Contacto
T. 948 194 888
info@itracasa.es
C/Cabárceno 6, 31621
Sarriguren, Navarra, España

www.itracasa.es
linkedin.com/company/tracasa-instrumental
@itracasa

tracasa instrumental

Gobierno de Navarra Nafarroako Gobernua

cpen

AENOR GESTIÓN AMBIENTAL ISO 14001

TÜVRheinland CERTIFICADO Sistema de Gestión ISO/IEC 27001:2013 www.tuv.com ID 9108641606