noanet
Soluciones de T.I.

SMARTFENSE

Caso de éxito

HACIA UNA CULTURA CIBERSEGURA

En solo 2 años, Noanet logró mejorar los hábitos de sus usuarios gracias a las campañas de concientización en ciberseguridad de SMARTFENSE.

noanet Soluciones de T.I. SMARTFENSE

El usuario ya no cae en las trampas, aún cuando quizás pueda abrir el email. Los usuarios ya no hacen clic en los links o no descargan archivos maliciosos.
Además, muchos se comunican con el área de IT para reportar los casos sospechosos. Esto muestra en forma directa la conducta responsable y los cambios de hábitos.

Jorge Gallardo

Responsable de Seguridad
de la Información de Noanet

Hacia una cultura Cibersegura

Sobre Noanet

Con presencia en Jujuy y Tucumán (Argentina), Noanet es una empresa dedicada al desarrollo de soluciones TIC para todo tipo de organizaciones. Forma parte del grupo energético Fundación Noroeste, integrado por 5 compañías del norte argentino, con más de 1500 agentes.

La necesidad de concientizar

En 2012, el grupo lanzó una política de Seguridad que establecía que la información debía ser abordada como un activo de la compañía. Ante esta nueva definición normativa, las personas del grupo debían ser incluídas en un proceso de formación. La problemática residía en la dispersión de los agentes en las diferentes subsidiarias localizadas en dos provincias, con una cobertura de 700 km2.

Para 2016 la empresa ya había generado procesos de formación personalizados, con grandes esfuerzos y horas de dedicación. Se dictaban algunos cursos presenciales y se enviaban emails periódicos. En aquel momento, surgió la oportunidad de buscar otras herramientas que facilitaran la tarea. Se hizo un sondeo y se contactaron con diferentes empresas del cuadrante de Gartner, muchas de ellas en Estados Unidos. Coincidió que también conocieron a SMARTFENSE, y lo incluyeron entre las opciones a evaluar.

En la matriz de 2017 se tenían en cuenta los siguientes aspectos:

- La provisión de contenidos predefinidos sobre ciberseguridad.
- La posibilidad de personalizar los contenidos y los textos de la plataforma.
- El idioma. Los proveedores extranjeros declararon que podían adaptarse al lenguaje local, pero en Noanet notaron que se trataba de un español neutro, lejano a las terminologías y usos propios de la región.
- La modalidad de pago y las posibilidades de negociación.
- La autenticación con Active Directory. Este punto era muy importante, ya que los usuarios se logueaban con sus credenciales de negocio una única vez para todos los sistemas.

Algunas ventajas de SMARTFENSE

La integración de SMARTFENSE fue un hito para el grupo Fundación Noroeste, por ser su primera aplicación SaaS. La plataforma posibilitó la utilización de otros browsers, habilitando a los usuarios, sobre todo en mandos medios, a continuar sus procesos de concientización desde sus hogares. Sobre las funcionalidades, Noanet destaca la provisión de contenidos predefinidos como la característica más importante, en tanto disminuye significativamente los esfuerzos dedicados a la creación de los materiales. La posibilidad de personalizar y adaptar los contenidos es otro de los grandes diferenciales, ya que permite a Noanet ajustar las terminologías a sus políticas internas de Seguridad. Otra de las bondades de la plataforma, según Jorge Gallardo, es la vasta cantidad de versiones.

> *Es una virtud que no la he visto en ninguna otra compañía de software. Es un gran placer para mí interactuar con una empresa tan profesional como SMARTFENSE, porque se percibe la sensibilidad en el tema de Seguridad de la Información.*

Jorge Gallardo

Una implementación en semanas

Las evaluaciones se retomaron en abril de 2018. SMARTFENSE garantizaba la personalización de contenidos, la posibilidad de gestión de múltiples instancias desde un único portal, y la autenticación con las mismas credenciales. Además, ofrecía una guía para armar un plan de concientización desde el momento cero.

Todas estas bondades fueron cruciales para que Noanet llegara a la decisión final. Pocas semanas después ya se estaban lanzando campañas de simulación de Phishing y Ransomware para grupos reducidos. Noanet tenía la intuición de que había algunos usuarios conscientes de los peligros y otros no. Los resultados ayudaron entender el estado inicial de la empresa, comprobando que muchos colaboradores, incluso en los altos niveles jerárquicos, caían en las trampas.

De esta forma, se pudo demostrar al directorio que se debía transitar un proceso de formación, acompañando a los usuarios para que aprendieran a identificar las amenazas que llegaban en los correos electrónicos.
Pronto se definieron campañas de concientización con módulos interactivos, sumando envíos semanales de newsletters. Los objetivos eran:

1) Exponer las políticas de Seguridad de la Información de la empresa.
2) Generar hábitos seguros en los usuarios. Jorge recuerda que el primer tema a desarrollar fue “Navegación Segura”.
Una vez alcanzado cierto nivel de madurez en 2019, Noanet logró formalizar un plan de concientización con acciones mensuales: módulos interactivos y newsletters, más simulaciones de Phishing y Ransomware alternadas.
A eso sumaban diferentes Momentos Educativos que se presentaban a cada usuario que caía en una trampa.

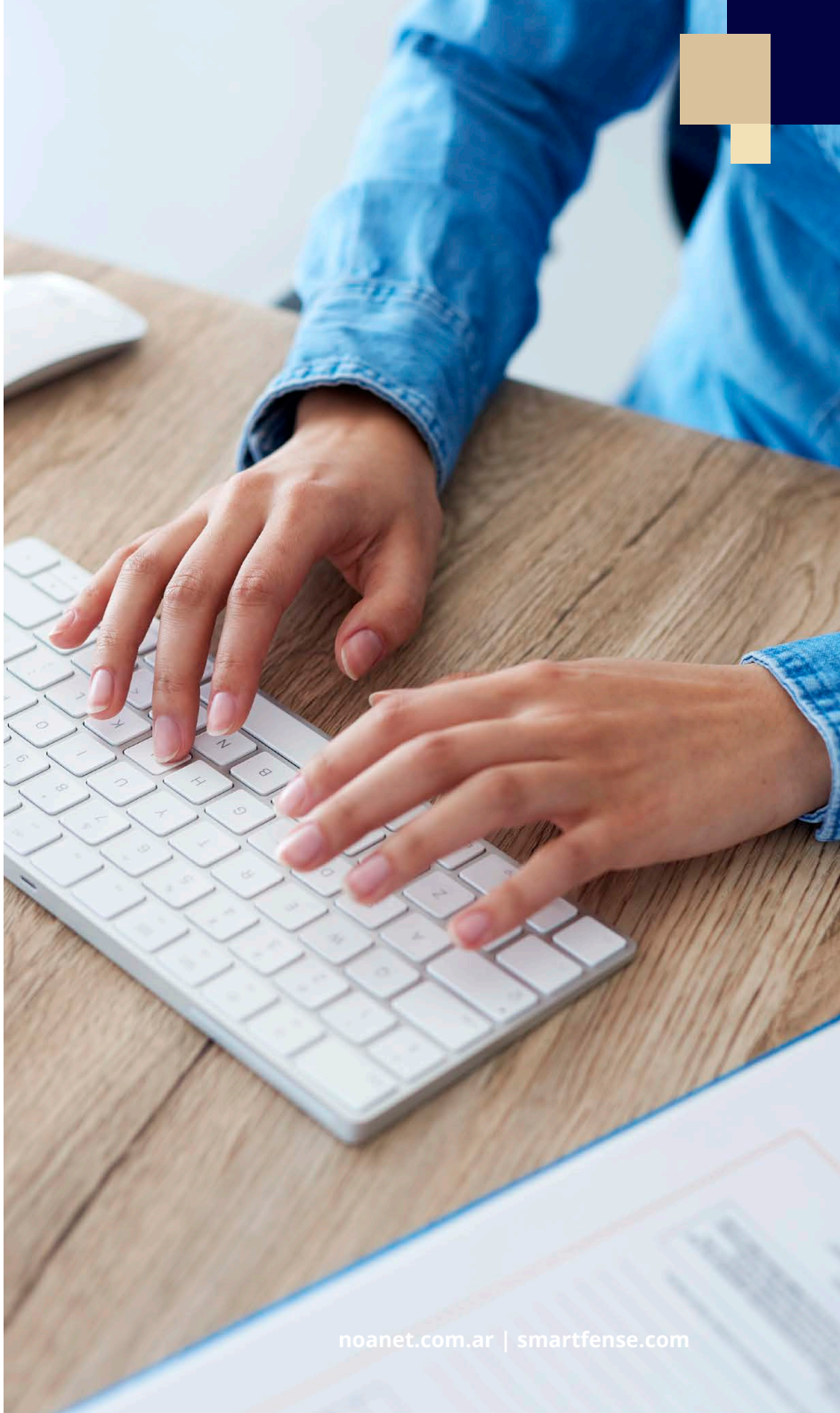
Los mejores resultados

Gracias a la presentación de los resultados de las campañas mediante las auditorías y los reportes, los integrantes del área de Seguridad de la Información pudieron detectar comportamientos no deseados, así como notar que había un entendimiento cada vez mayor sobre las cuestiones de Ciberseguridad.

"A veces no habíamos ajustado el contenido a una política, y las personas lo alertaban. Eso demostraba que la gente prestaba atención y usaba la plataforma, más allá de los indicadores que se obtenían de los reportes", declara Jorge Gallardo.

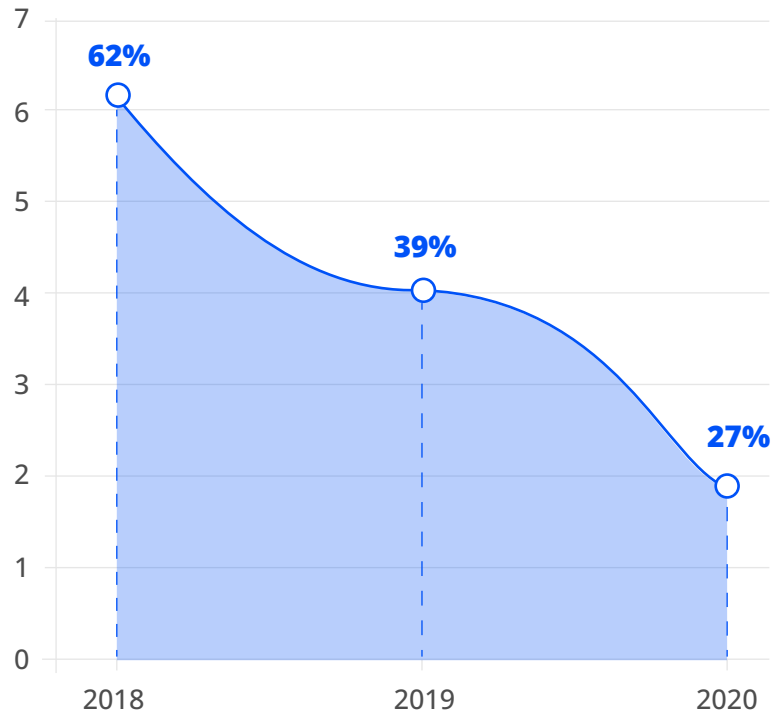
Las auditorías por campañas y por usuarios permitieron hacer seguimientos personalizados ante casos puntuales que continuaban "mordiendo el anzuelo". Pero muchos de los colaboradores del grupo empezaron a dar aviso sobre ciertos correos que recibían, marcándolos como SPAM. Gracias a los reportes automáticos de la herramienta, los líderes del proyecto podían presentar informes bimestrales a la alta gerencia para demostrar la progresión y la mejora en los hábitos de los usuarios.

"Los usuarios ya no hacen clic en los links o no descargan archivos maliciosos. Además, muchos se comunican con el área de IT para reportar los casos sospechosos. Esto muestra en forma directa la conducta responsable y los cambios de hábitos", concluye Jorge.



Evolución del comportamiento de los usuarios

(según los resultados de simulaciones de Phishing)



*Porcentaje de usuarios que cayeron en trampas simuladasde Phishing.

Evolución del comportamiento de los usuarios

(según los resultados de simulaciones de Phishing)

2018

61% de los usuarios
cayeron en las trampas.

2019

39% de los usuarios no reconocieron los emails maliciosos.

Después de un año de lanzar campañas de módulos interactivos y newsletters

2020

Los comportamientos riesgosos se redujeron al 27% sobre el total de acciones de los usuarios

Luego de otro año continuando con el plan de concientización en Seguridad de la Información, iterando contenidos y sumando nuevos tópicos personalizados.

info@smartfense.com | smartfense.com