UNIVERSIDAD NACIONAL DE TUCUMAN
FACULTAD DE CIENCIAS ECONÓMICAS

Seguridad y Control
en Sistemas Informáticos

¿CÓMO FORTALECER UNA CULTURA DE SEGURIDAD DE LA INFORMACIÓN A TRAVÉS DE LA CONCIENTIZACIÓN?
ESTUDIO DE CASO EN EMPRESA TUCUMANA

ACEÑOLAZA CHAMORRO, INÉS
ALEXANDER, FRANCO MATÍAS
HASKOUR, ARIANA MARÍA
VENDITTI GALO, FLORENCIA

NOVIEMBRE 2022

PROFESOR: MARCELO GARCIA

Declaración jurada

"Por medio de la presente, los autores manifiestan conocer y aceptar el "Reglamento para la Presentación de Trabajo Final" vigente de la asignatura "Seguridad y Control en Sistemas Informáticos", haciéndose responsables por la totalidad de los contenidos del presente documento, los cuales son originales y de creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación nacional e internacional de Propiedad Intelectual"

FIRMADO
Aceñolaza Chamorro, Inés
Alexander, Franco Matías
Haskour, Ariana María
Venditti Galo, Florencia

TABLA DE CONTENIDOS

1. RESUMEN

En el marco de la materia Seguridad y Control de Sistemas informáticos se realizó el presente trabajo a los efectos de poder aplicar los conocimientos adquiridos durante el cursado. El objetivo general de esta investigación es relevar el proceso de concientización en seguridad de la información de la empresa tucumana SyC, haciendo énfasis en la importancia de contar con recursos humanos capacitados en el tema.

El trabajo efectuado se realizó con un relevamiento de datos a través de distintos métodos entre ellos una sesión de profundidad, participando en un seminario dictado por la responsable de Seguridad de la Información en la empresa bajo estudio. Otros métodos fueron muestra de expertos, revisión de documentos y datos secundarios.

Para el análisis y desarrollo del proceso de fortalecimiento de concientización se dio uso a una herramienta llamada “SmartFense” con la finalidad de analizar datos dentro de la empresa a partir de campañas efectuadas para evaluar el grado y nivel de riesgo que se maneja dentro de la misma. De acuerdo con lo analizado y los resultados vistos, se llevará a cabo una serie de recomendaciones para la implementación dentro de la empresa SyC y también fuera de ella, nombrando herramientas útiles para cualquier empresa que quiera iniciarse o esté en proceso de fortalecimiento de la concientización en la cultura de seguridad de la información.

2. INTRODUCCIÓN

En los últimos años se hizo evidente el crecimiento de la tecnología de la información en el área empresarial. La incorporación de las TIC en este ámbito puede resultar un elemento clave para mejorar la competitividad e impulsar el crecimiento económico. De la misma forma, se multiplicaron los delitos cibernéticos, que van más allá del robo de información, volviéndose cada vez más lucrativos.

Según Ahlgren, M (20 de octubre 2022). “Se estima que el costo global anual por ciberdelincuencia será de $10.5 U$D billones para el año 2025”. Como consecuencia la gestión de la seguridad de la información tomó un papel fundamental y con ello las personas involucradas.

Cuando hablamos de seguridad, instintivamente pensamos en herramientas o procedimientos de seguridad, pero en realidad, la seguridad depende de un factor común a cualquier entidad: los empleados. De ellos depende en gran medida el éxito o fracaso de la implantación, ya que son los encargados de gestionar nuestro principal activo: la información. “El 85% de las infracciones de seguridad cibernética son causadas por errores humanos”.

Invertir en la formación y concienciación a los empleados debe ser una actividad recurrente, a fin de desarrollar una cultura de seguridad, ya que, por muchos resguardos que se tomen, si la concientización no es permanente en el interior de las organizaciones, lo más probable es que se termine dentro de los

crecientes porcentajes de víctimas de ciberdelincuencia. Efectivamente, la tecnología por sí sola no puede mantenernos seguros.

Pero, ¿Cómo impacta un ataque informático dentro de la empresa Tucumana SyC? Para responder esa pregunta, hay que tener en cuenta que esta empresa es un monopolio de servicios públicos, por lo que el impacto no se vería arraigado sobre la imagen de la misma. Un ataque informático de cualquier forma tendría un gran impacto en la sociedad, al no poder cumplir con las necesidades y demandas del mercado.

Un ataque de ingeniería social, un ransomware o incluso un phishing pueden llegar a costar mucho para las empresas, dejando inhabilitadas sus operaciones y con ello afectando a la comunidad.

3. PLANIFICACIÓN DE LA INTERVENCIÓN Y SU SEGUIMIENTO.

El Ministerio de Ciencia, Tecnología e Innovación, asegura que Argentina es el país que más invierte en tecnología de la información en la región, pero, ¿De qué sirve invertir mucho dinero en tecnología, si las personas dentro de la organización siguen siendo el eslabón más débil en el área de seguridad?

Un programa de concientización y capacitación en seguridad es sumamente importante para las empresas, ya que un empleado puede no ser malicioso de manera intencionada, pero no conocer cuáles son los procedimientos adecuados o caer en las trampas de los ciberdelincuentes.

La creación de una cultura de conocimiento de la ciberseguridad es un esfuerzo continuo que requiere el liderazgo de la administración superior y el compromiso de todos los usuarios y empleados.

El objetivo general de esta investigación es relevar el proceso de concientización en seguridad de la información de la empresa tucumana SyC, haciendo énfasis en la importancia de contar con recursos humanos especializados en el tema.

Los objetivos específicos son:

-Conocer en profundidad la herramienta SmartFense e indagar en herramientas alternativas.

-Ofrecer a la empresa recomendaciones, verificando su eficiencia, para continuar fortaleciendo su cultura.

-Detallar un plan de acción a seguir, para empresas iniciándose en el tema, con el objetivo de fortalecer la cultura de concientización en seguridad de la información

Así, el alcance de esta investigación se limita a relevar información sobre el proceso implementado para la capacitación y concientización de la empresa Tucumana SyC, monopolio de servicios públicos.

4. MARCO TEÓRICO

Se puede definir a la **seguridad de la información** como: “La disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de

proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta". La seguridad de la información parte de la premisa de que los datos son el nuevo gran valor y tesoro de la nueva realidad, ya que los malos manejos que se puedan hacer con ella, pueden ser catastróficos, para gobiernos, empresas e incluso para las personas que manejan datos delicados en línea.

Las **tecnologías de la información y la comunicación o TIC** corresponden y se refieren a todas las tecnologías que de una u otra forma interfieren y median en los procesos informacionales y comunicativos entre seres humanos, y pueden ser entendidas como un conjunto de recursos tecnológicos integrados entre sí, que proporcionan, por medio de facilidades de hardware, de software, y de telecomunicaciones, la semi-automatización y comunicación de procesos relativos a negocios, a investigación científica, a enseñanza, a aprendizaje, a cuestiones de la vida diaria, etc.

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Que una empresa sea certificada significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. Se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

El uso de la palabra **"cultura"** es importante para comprender este trabajo. Una cultura abarca ideas, costumbres y, sobre todo, comportamientos. El comportamiento humano está detrás de muchas violaciones de datos accidentales, especialmente las que implican phishing. Para acabar con esto y sustituirlo por una cultura de conocimiento y comprensión de cómo interactúan la ciberseguridad y el cumplimiento de la normativa, hay que empezar por la cúpula y dispersarse por toda la organización. Esto es lo que conocemos como **"cultura de concientización en seguridad de la información".** La misma es uno de los mecanismos más importantes para influenciar el comportamiento de los empleados en cuanto a ciberseguridad.

La herramienta **SmartFense** es una plataforma de capacitación y concienciación en Seguridad de la Información que genera hábitos seguros en los usuarios finales. Para lograrlo integra herramientas de diversos tipos como: evaluación, auditoría y compliance, educación y esfuerzo, y medición.

5. MARCO METODOLÓGICO

Se abordará el trabajo desde un enfoque cualitativo con diseño no experimental de tipo descriptivo ya que recurre al estudio de un caso de forma intensiva. Se busca analizar el proceso de concientización de seguridad de la información en la empresa recopilando datos a través de los siguientes métodos:

- Sesión en profundidad: mediante la participación en un seminario, donde se recolectará información para comprender el accionar diario de la empresa.
- Entrevista a expertos: realizada al responsable de seguridad de la información de la empresa para profundizar sobre la forma en la que se lleva a cabo la capacitación y concientización a empleados.
- Revisión documental: se accederá a la política formal de la empresa y a material adicional sobre los sistemas.
- Datos secundarios: se investigarán posibles alternativas de herramientas para facilitar y potenciar las campañas de capacitación.

Etapas de investigación

1. Estudio bibliográfico;
2. Inmersión en la empresa de estudio;
3. Recolección de los datos a través de las diversas técnicas mencionadas;
4. Revisión y análisis de datos;
5. Valoración del proceso de concientización en seguridad de la información en la empresa;
6. Presentación de conclusiones y de herramientas alternativas para la capacitación.

6. RECOLECCIÓN Y ANÁLISIS DE DATOS:

● 6.1 SEMINARIO DICTADO POR LA RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA.

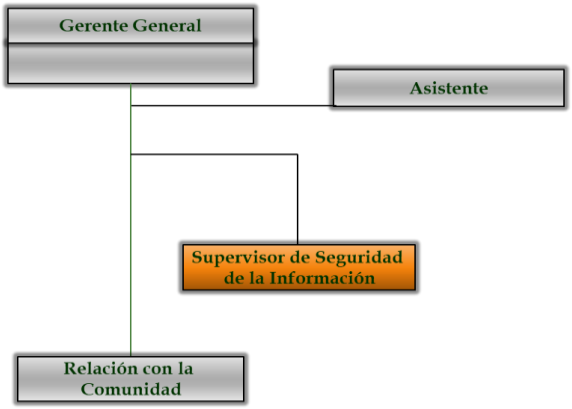
El día martes 25 de octubre del 2022, en el marco de la asignatura Seguridad y Control de Sistemas Informáticos, se tuvo la posibilidad de asistir al seminario “El día a día de la seguridad de la información en una empresa tucumana” dictado por el responsable de la Seguridad de la Información de la empresa.

Del mismo se pudo recabar la siguiente información:

Existe en la empresa un supervisor de seguridad de la información que depende directamente de la gerencia general. El área sólo está integrada por el responsable de seguridad de la información, debido a que la empresa terceriza todos los servicios informáticos. Este responsable está encargado de investigar, desarrollar, proponer y mantener las políticas y procedimientos de Seguridad de la Información, como así también de participar activamente de la gestión de incidentes y gestión de cambios de los activos de información a fin de maximizar la generación de valor, aportando a la gestión de riesgos, control y gobierno corporativo.

A continuación, se presenta un organigrama que refleja dicha relación.

Gráfico 1: Organigrama



Fuente: Presentación del disertante.

Se pudo identificar las políticas de seguridad de información que se llevan a cabo en la empresa, basándose en el objeto principal de proteger y garantizar los aspectos de confidencialidad, integridad y disponibilidad de la información de acuerdo a los requerimientos del negocio.

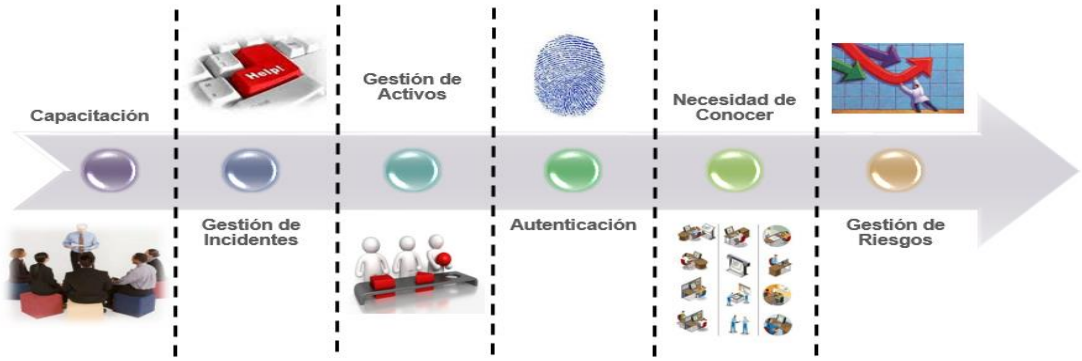
Para poder desarrollar estas políticas de seguridad es necesaria la formación de un equipo de trabajo con la participación activa de propietarios y custodios a fin de implementar los pilares básicos. Para ello, existe un comité de seguridad encargado de facilitar la toma de decisiones no incluidas dentro de la política de la empresa, conformado por la alta dirección de la empresa.

Los aspectos considerados para la política de seguridad son:

- El manejo consistente de la información
- Acceso a información en base a la necesidad
- Autenticación de usuarios
- Uso personal de los recursos de la empresa
- Actividades no permitidas
- Informes obligatorios
- Derechos sobre el material Desarrollado

Para la implementación se siguió un curso de acción basado en los siguientes pilares:

Gráfico 2: pilares de la seguridad de la información de la empresa



Fuente: Presentación del disertante.

El primer pilar resulta crucial para sostener a los demás. La capacitación inicial debe ser hacia supervisores, jefes y gerentes. La misma se logra a través de campañas, que inician con la realización de Métricas para saber la situación actual en la que se encuentra la empresa. A partir de estas se ponen en marcha las capacitaciones necesarias que luego serán comparadas con las métricas para un posterior análisis de resultados. Con esto se puede implementar refuerzos de campaña sabiendo los puntos débiles que deben reforzar y así comenzar de nuevo el ciclo.

Con respecto a la gestión de incidentes, la empresa realiza reuniones mensuales para evaluar los posibles riesgos y buscar la mejor manera de abordarlos. Por cada incidente producido se realiza un informe detallando el impacto generado en el negocio.

Sobre el pilar de Gestión de activos, se construye un inventario de activos que se va actualizando a medida que se aumentan o disminuyen estos activos de información. Esta base cumple con la Ley de Protección de Datos Personales (Ley 25326).

La empresa requiere que cada empleado y tercero que accede al sistema tenga un único identificador y sea responsable por el uso del mismo. Las contraseñas de los usuarios deben ser de uso personal e intransferible, por lo que la empresa cuenta con una política de autenticación de contraseñas fuertes y con un doble factor de autenticación.

El acceso a información de la empresa se proporciona de acuerdo al pilar Necesidad de Conocer. El mismo hace referencia a que la información debe ser divulgada únicamente a las personas que tengan una necesidad legítima sobre esta. Es por esto que la empresa se centró en redefinir los roles de acceso y formalizar una gestión corporativa de los permisos de acceso a información.

El pilar de la Gestión de Riesgos todavía no se encuentra implementado en la empresa. Se está buscando un sistema integrado a la gestión de cambios, gestión de incidentes y basándose en la gestión de activos.

El presente trabajo se enfocará en el estudio del primer pilar de seguridad de la información en la empresa: la capacitación. Se analizará el proceso llevado a cabo y la herramienta utilizada para esto: SmartFense.

Para lograr el cumplimiento de los objetivos, se siguieron los siguientes pasos:

- Formalizar un equipo de trabajo
- Publicar formalmente la política de seguridad
- Aprobar un plan de acción
- Presupuestar el plan de acción
- Conocer la estrategia de adquisición de herramientas de seguridad
- Realizar reuniones periódicas de avance del proyecto

● 6.2 ENTREVISTA:

Se tuvo la oportunidad de entrevistar al responsable de seguridad de la información, a través de una entrevista no estructurada con preguntas abiertas, dando lugar al diálogo continuo e inmersión en nuevos temas relacionados. Se recolectó la siguiente información:

La capacitación tiene mucha importancia en todas las áreas de la empresa, es por esto que cuentan con un área de RRHH especializados en capacitar.

Se considera que la seguridad de la información se mide a través del eslabón más débil, los recursos humanos. Por lo que, la concientización forma parte de los pilares básicos de seguridad de la información en la empresa.

Lo primero que se realizó en la empresa hace 10 años fue definir una Política de Seguridad, para que los usuarios tengan el conocimiento de esta. En ese entonces, no se implementó ninguna herramienta de apoyo informática, por lo que todas las capacitaciones posteriores a la política se hicieron de manera presencial y periódicas dirigidas el personal de la empresa, como así también a las empresas contratistas que tenían uso de información de la propia empresa. La forma de evidenciar estas capacitaciones presenciales, era con la realización de pequeños exámenes que constaban de dos o tres preguntas sobre lo aprendido, a todos los empleados que las hubiesen presenciado. Este proceso se dificultaba ya que contaban con más de 1500 empleados.

Actualmente se implementó la herramienta de seguridad “SmartFense” para facilitar el dictado de capacitaciones. Debido a la eficacia de la herramienta, posteriormente se incorporó en las distintas áreas y procesos de la empresa. Dicha herramienta cuenta con distintos módulos y ofrece diversos métodos, entre ellos, módulos interactivos, newsletter, videojuegos, phishing y ransomware. También brinda la posibilidad de personalizar dichas capacitaciones. Otra gran utilidad, es que proporciona reportes de auditoría y estadísticas sobre los instrumentos utilizados dentro de la herramienta, que son de gran utilidad para evaluar el impacto de cada una en los procesos de la empresa.

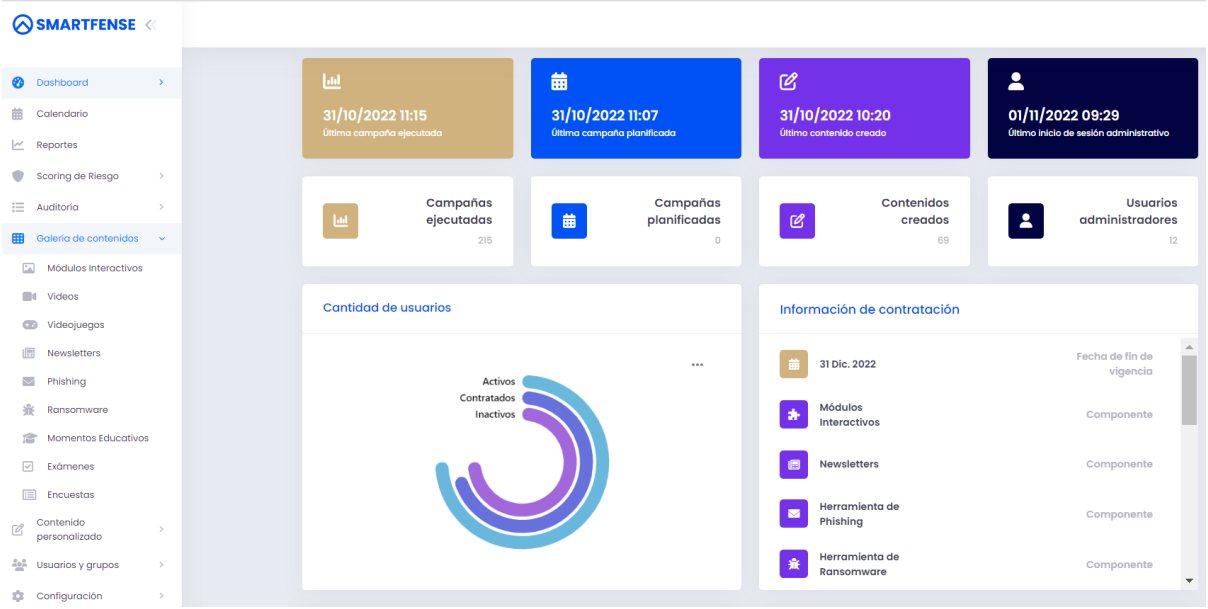
Esta herramienta tiene una relación estrecha con el control de gestión, facilitó la incorporación de métricas que permiten medir las horas hombres acumuladas, de cada empleado, a través de insignias o logros. Las insignias obtenidas por el cumplimiento de las capacitaciones, se refleja en los indicadores de “seguridad de la información” para medir la adhesión en las mismas de cada uno de los usuarios. Luego se informa a cada jefe de área para que este replique indicaciones a su personal a cargo, definiendo un plan de acción.

Estas capacitaciones se llevan a cabo en el proceso de inducción de nuevos empleados y también es enviada a aquellos a los no fueron capacitados anteriormente. No se logra una adhesión a las capacitaciones del 100%, pero se intenta disminuir esta brecha realizando, una vez al año, una Jornada de Seguridad de la Información invitando a toda la empresa, de forma opcional.

Durante el transcurso del 2022, se implementaron cambios en la forma de brindar las jornadas, invitando a personas externas a la organización, sobre temas relacionados a la Seguridad de la Información. Entre ellas, una mesa panel con la temática ”yo tuve un incidente de seguridad”, para realizar un relevamiento sobre experiencias de usuarios y casos para la discusión.

Actualmente, no se puede afirmar que la empresa cuenta con una cultura de concientización en seguridad de la información establecida, pero se está trabajando constantemente para lograrlo: fomentar la conciencia a través de pequeños hábitos.

Gráfico 3: dashboard de SmartFense

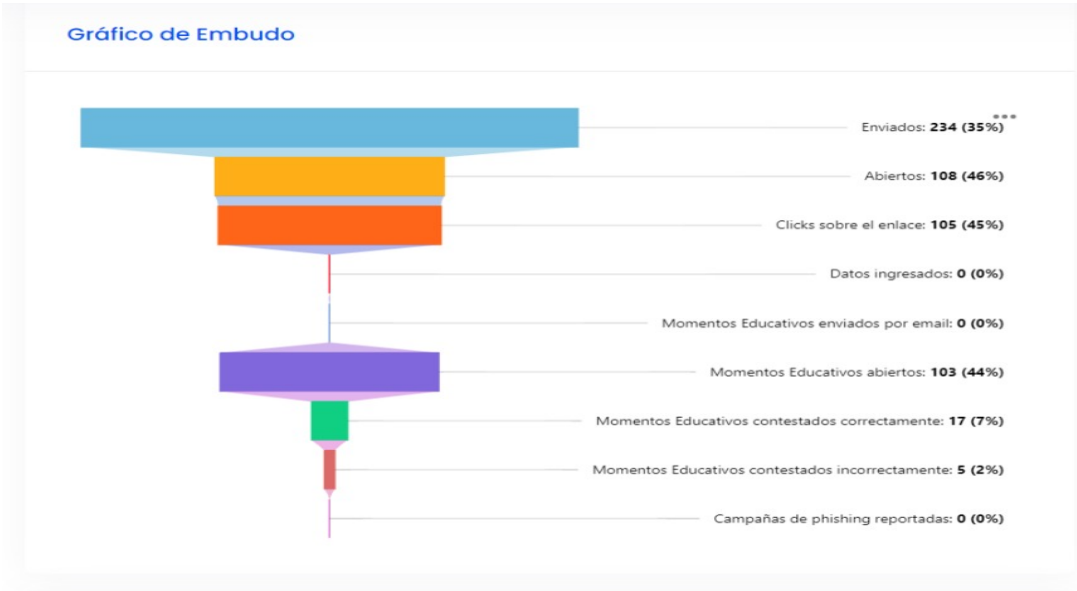


Fuente: captura de pantalla del disertante

- **6.3 DOCUMENTOS**

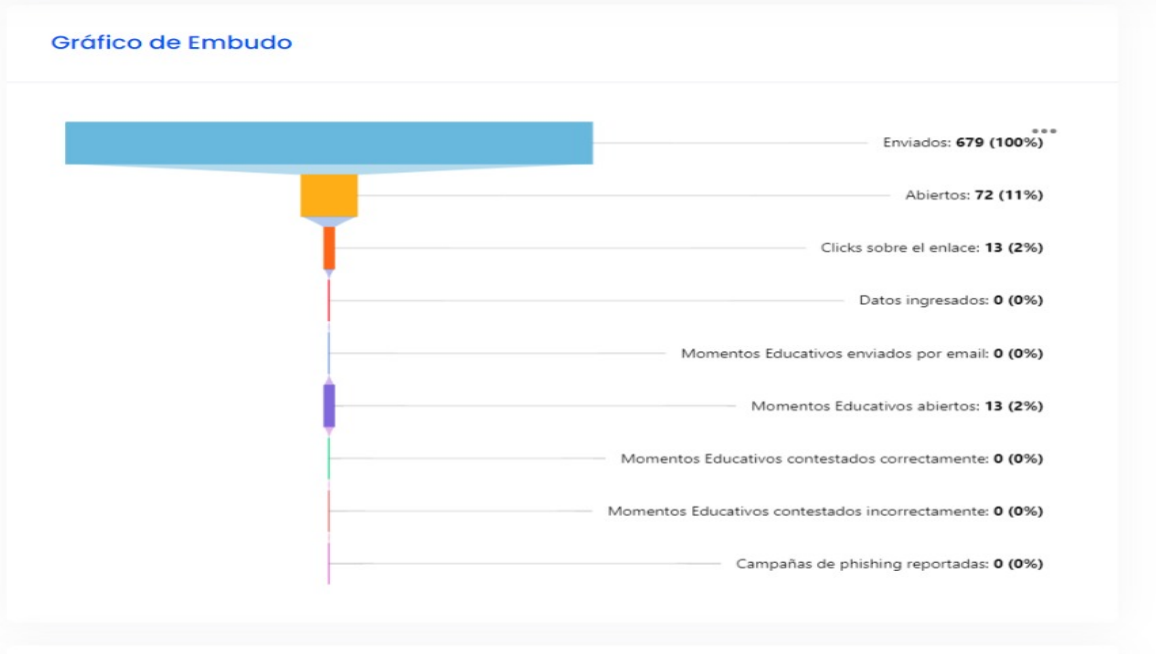
Se presentan los resultados de campañas de phishing realizadas por la responsable de Seguridad de la información en SyC mediante el uso de la herramienta SmartFense en dos fechas distintas:

Gráfico de embudo 1:
Fecha de inicio: 14/08/2019
Tópico/Escenario: OCA: ¡Tu paquete está listo para retirar!



Se puede observar que, casi un 50% de los empleados que recibieron el mail, abrieron y clickearon sobre el enlace. Debido a esto, un 21% de los mismos accedieron a un “Momento educativo” donde se intentan corregir estas desviaciones. Posteriormente, se realiza un examen sobre lo aprendido, y como se muestra en el gráfico, solo el 22% contestaron las preguntas planteadas.

Gráfico de embudo 2:
Fecha de inicio: 10/10/2022
Tópico/Escenario: Adidas: Qatar 2022, ¡Ganate la pelota del mundial!



Se puede observar que, esta vez, un 11% de los empleados que recibieron el mail, lo abrieron, pero solo el 2% clickeo sobre el enlace. Este 2% accedió al momento educativo, pero ninguno realizó el examen correspondiente.

- ## 6.4 DATOS SECUNDARIOS

Se realizó una búsqueda de herramientas gratuitas útiles para facilitar concientización sobre seguridad de la información dirigida a recursos humanos.

6.4.1 GO PHISH

Una herramienta para la simulación de ataques de phishing y con ella podrás realizar entrenamiento de técnicas de Phishing. Se trata de un sistema de phishing de código abierto destinado a poner a disposición de cualquier persona/empresa/compañía el entrenamiento.

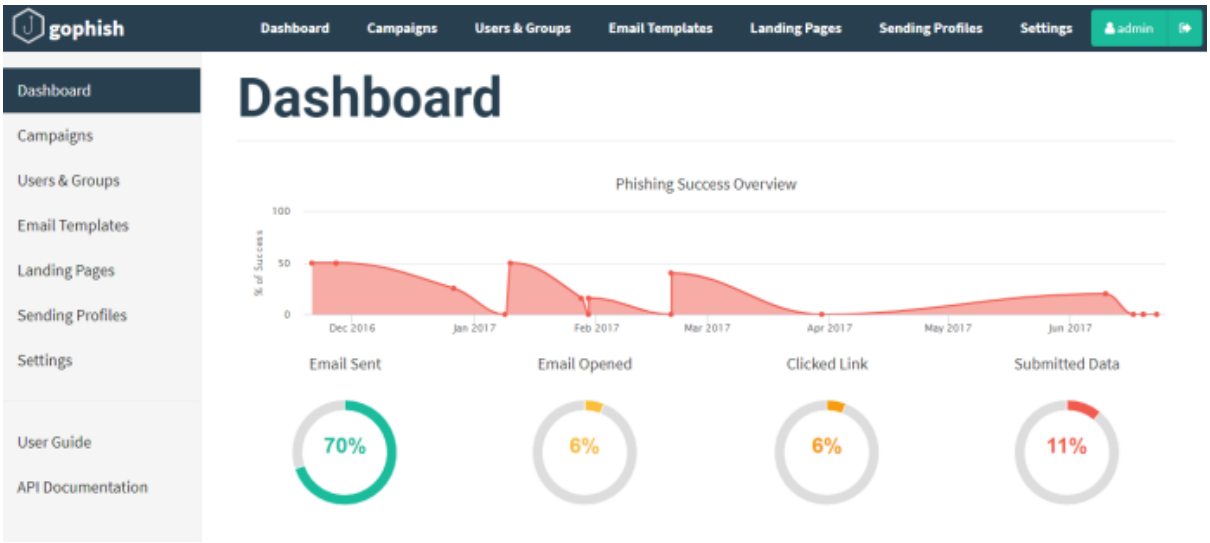
Sus principales virtudes son:

- Es de código abierto y gratuito.

- Está escrito en el lenguaje de programación Go, por lo que es «descargar y jugar».
- Se encuentra alojado en la red interna de la compañía, evitando fugas de información.

Posee una interfaz muy sencilla y permite que los administradores de sistema automaticen, sin complicación alguna, sus propias simulaciones de phishing.

Gráfico 4: dashboard "Go Phish"



Fuente: Go Phish

6.4.2 KNOW BE4

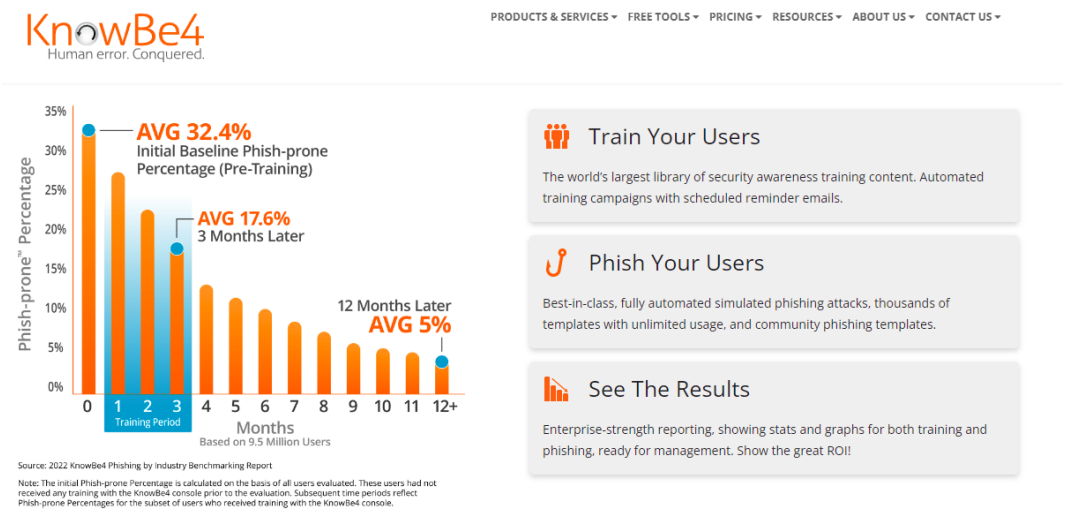
KnowBe4 es la plataforma integrada más grande del mundo para la capacitación en concientización sobre seguridad combinada con ataques de phishing simulados.

Proporciona pruebas de referencia para evaluar el porcentaje de usuarios propensos al phishing a través de un ataque de phishing simulado gratuito .
Posee la biblioteca más grande del mundo de contenido de capacitación sobre seguridad; incluyendo módulos interactivos, juegos, carteles, boletines y campañas de formación automatizadas con correos electrónicos de recordatorio programados.

Ofrece también Informes de solidez empresarial, que muestran estadísticas y gráficos tanto para la capacitación en concientización sobre seguridad como para el phishing, listos para la administración.

Con la función de grupos inteligentes, se puede usar el comportamiento de cada empleado y los atributos de usuario para personalizar campañas de phishing, tareas de capacitación, aprendizaje correctivo e informes.

Gráfico 5: Servicios de KnowBe4



Fuente: KnowBe4

7. CONCLUSIONES Y RECOMENDACIONES

A partir del relevamiento del proceso de concientización en seguridad de la información de la empresa bajo estudio, se puede concluir que la misma está en proceso de fortalecimiento de su cultura de concientización. Cuenta con los recursos suficientes para hacer frente a las diferentes situaciones que se van presentando y el responsable tiene a su disposición presupuesto, herramientas y recursos humanos destinados específicamente para concientización.

A pesar de que SyC no está certificado en ISO 27001, se puede apreciar que cumple con los requisitos para lograrlo. La norma exige que las personas dentro de la organización tengan conocimiento de:

- **La política de seguridad de la información:** cada vez que ingresa un empleado, la empresa realiza un fuerte proceso de inducción en el cual se muestran videos interactivos sobre los distintos puntos que abarca la política de seguridad. Además, se entrega el documento formal de la misma a cada empleado y se exige al mismo manifestar su conocimiento a través de su firma.
- **Su contribución a la eficacia del Sistema de Gestión de la Seguridad de la Información (SGSI):** a partir de capacitaciones se da a conocer a los empleados de los diferentes puestos su aporte al sistema.
- **Las implicancias de no cumplir con los requisitos del SGSI:** para cada puesto de trabajo se realizó una evaluación de riesgos donde se dan a conocer las vulnerabilidades a las que se encuentran expuestos y el impacto que generaría en el negocio.

En base a los documentos analizados de la empresa sobre las campañas de phishing implementadas en el personal de la organización a aquellos empleados que tienen acceso a la red y a los sistemas de la empresa, utilizando la herramienta SmartFense, se llegó a la conclusión que las acciones destinadas a la

concientización en la seguridad de la información tuvieron un efecto positivo, disminuyendo la brecha entre las indicaciones brindadas en las capacitaciones y los conocimientos adquiridos.

Se recomienda a la empresa categorizar, mediante perfiles informáticos de puestos, a los empleados en función a sus actividades y determinar el nivel de riesgo al que se encuentran expuestos, agrupando por áreas operativas, gerenciales y de alta jerarquía. Para cada grupo se debe evaluar el nivel de riesgo según sea “intolerable”, “alto”, “medio”, “bajo” o “libre de riesgo”, y fijar estándares de errores “aceptables” e “inaceptables” con las medidas correctivas asociadas.

También se considera necesario la realización de reuniones periódicas con el grupo expuesto a riesgo “intolerable” y “alto” para lograr una mayor profundidad en la concientización sobre seguridad de la información evitando así potenciales perjuicios para el normal funcionamiento de la empresa.

Teniendo en cuenta el camino recorrido por SyC, se propone a las empresas iniciándose en el proceso de concientización en seguridad de información, considerar previamente los siguientes puntos fundamentales:

- Crear un área de Seguridad de la Información y designar un responsable que tenga conocimiento sobre los aspectos clave de la misma.
- Identificar la información que exige protección y establecer el valor de esa información en términos de costos.
- Lograr compromiso de parte de la dirección, presentando los riesgos e impactos de posibles amenazas, con el fin de obtener recursos necesarios.
- Redactar una política de seguridad de la información, acorde a las características del negocio, y objetivos a cumplir en distintos plazos.

Una vez definidos estos aspectos claves para la seguridad, es recomendable proceder con la comunicación y concientización a los recursos humanos de la empresa. Para ello se propone:

- Comunicar las políticas y objetivos fijados a toda la organización mediante videos interactivos y entrega del documento formal, solicitando la firma de cada empleado manifestando su comprensión.
- Elaborar un plan de capacitaciones acorde a las necesidades de la empresa. Posteriormente realizar capacitaciones en base al mismo. Se proponen algunos temas de interés: Escritorios limpios. Contraseñas seguras. Autenticación.
- Implantar una herramienta de seguridad: una buena alternativa inicial y gratuita es GO PHISH mediante la cual se puede enviar phishing a cada empleado de la empresa y evaluar los efectos de las capacitaciones previas. A medida que la empresa vaya creciendo en el área, se pueden aplicar algunas herramientas con mayores funcionalidades como KnowBe4 que ofrece más funciones gratuitas. SmartFense es la opción más completa analizada para gestionar campañas de capacitación; se recomienda tenerla en cuenta si el presupuesto destinado al área lo permite.

- Realizar “Jornada de la Seguridad de la Información” con incentivos, en donde se comunique continuamente la política de seguridad y se realicen juegos interactivos para familiarizarse con la misma.
- Establecer métricas para medir la eficiencia de las acciones tomadas e impulsar el desarrollo de nuevas medidas.

8. BIBLIOGRAFÍA

- Ahlgren, M (20 de octubre 2022). *MÁS DE 40 ESTADÍSTICAS Y HECHOS DE CIBERSEGURIDAD PARA 2022.* https://www.websiterating.com
- Martin, B. (1 de octubre 2019) *La importancia de la concienciación en la seguridad de la información. Informe Internet de las cosas: La tecnología como aliada de la sostenibilidad* https://dpd.aec.es/la-importancia-de-la-concienciacion-en-la-seguridad-de-la-informacion/
- *Gallego Gomez, C (16 de septiembre 2022) Informe Internet de las cosas: La tecnología como aliada de la sostenibilidad.* https://www.argentina.gob.ar/noticias/argentina-es-el-pais-que-mas-invierte-en-tecnologia-de-la-informacion-en-la-region
- Olivera, M. I*mportancia de la concienciación en ciberseguridad. Recuperado Internet de: https://www.ciberseguridadlatam.com/2022/08/24/importancia-de-la-concientizacion-en-ciberseguridad/#:~:text=As%C3%AD%2C%20por%20muchos%20resguardos%20que,sola%20no%20puede%20mantenernos%20seguros*.
- Mackey, J. (8 de Julio 2021) *Creación De Una Cultura De Cumplimiento De La Ciberseguridad. https://www.metacompliance.com/es/blog/cyber-security-awareness/compliance-culture*
- *AdminIberoBlogs. (10 de Julio 2020) La importancia de la seguridad de la información.* https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/
- Urbina Baca, G (2016) *Introduccion a la seguridad informática.*
- Cisco Networking Academy (2016) *Cibersecurity Essentials*
- *Derechodelared (25 de abril 2022) Gophish, la herramienta para entrenar usuarios contra el phishing. https://derechodelared.com/gophish/*
- https://advisera.com/27001academy/es/que-es-iso-27001/
- HelpNetSecurity (11 de mayo 2017) *La cultura es más útil que la concientización en seguridad informática*. https://www.cert.unam.mx/la-cultura-es-mas-util-que-la-concientizacion-en-seguridad-informatica

9. ANEXO

ENTREVISTA CON EXPERTO

¿Qué importancia se le da a la capacitación dentro de la empresa?

En la empresa se le da mucha importancia a la capacitación, no solo a la de seguridad en la información sino a todas las capacitaciones. Hay un área dentro de recursos humanos que está dedicada a esto y el fuerte es la capacitación en el

área técnica, que es el Core del negocio de la empresa. Entonces, teniendo este sector y las herramientas, fue muy fácil que nos autorice a comprar una herramienta específica para seguridad de la información y que se dicte la capacitación, porque ya hay un área especializada en esto. Por lo tanto, si, se le da mucha importancia, hay planes de capacitación y herramientas para facilitar la misma. El 30 de noviembre es el día de la seguridad de la información, siguiendo con esa fecha se organizan charlas, previamente la empresa elegía los temas y por medio de teams que es la herramienta que utilizan para reuniones, se invitaba a las personas , se daba la charla y para finalizar se realizaban preguntas, la herramienta SmartFense también puede hacer encuestas y evaluaciones, quien participaba de la charla y realizaba estas evaluaciones tiene doble chance de participar en un sorteos, premios relacionados a la tecnología.

¿Por qué consideran que es tan importante la capacitación?

Por qué se dice que la seguridad se mide por el eslabón más débil, y este eslabón son los recursos humanos. Uno puede invertir y tener muchos recursos de seguridad en la información, tanto de hardware como de software, pero si el usuario comparte la contraseña, ya no hay seguridad. Entonces la concientización y la capacitación a usuarios es lo más importante.

¿Se llevó a cabo en la empresa un proceso de educación y de concientización a los empleados?

Lo primero que se ha hecho en el área de seguridad ha sido definir la política de seguridad. Una vez definida, comenzó la parte de capacitación y hacer que todos los usuarios la conozcan y la firmen. Eso fue hace diez años. En ese momento no teníamos ninguna herramienta, por lo tanto, todas las capacitaciones fueron presenciales y fueron destinadas a todo el personal de la empresa, como así también a las contratistas que manejan información de la empresa.

Para dejar evidencia de la capacitación realizada, no sólo se firmaron las políticas, sino que se contestaron dos o tres preguntas referidas a la misma. Esto se hizo con los 1500 empleados. Actualmente ya no necesitamos hacer esa capacitación en forma presencial, ya tenemos el sistema que se llama SmartFense. Entonces, como parte de la inducción está la realización de esta capacitación, que son unos vídeos de seguridad de cada uno de los puntos de la política. Hay una introducción donde cuenta el objetivo de la política, las responsabilidades, a quienes alcanza la política y después un videíto sobre cada uno de los diez puntos específicos de la política.

¿En esas jornadas participa toda la empresa? ¿Es obligatorio?

Está invitada toda la empresa, no son obligatorias, se suman alrededor de 300 empleados que es muy poco para la cantidad que posee la empresa. Este año se implementaron algunos cambios, el principal cambio es que las charlas ahora las brindan personas de afuera de la organización, las charlas que se brindarán serán de grooming, que será ofrecida por un especialista de Jujuy, y la otra temática será sobre un viaje a Qatar, haciendo referencia a todas las publicidades

y demás temas relacionados a este. La tercera será una mesa panel con la temática “yo tuve un incidente de seguridad”, para realizar un relevamiento de que es lo que le paso a los usuarios y poner casos para discusión. Estas 3 conferencias se dan en un horario determinado la primera semana y en otro horario la segunda semana, para poder tener más adhesión de los usuarios

¿Se asegura que todos los usuarios estén capacitados e informados para cumplir sus deberes con respecto a la seguridad cibernética? ¿Cómo se hace?

Ayuda mucho el sistema que tenemos. El sistema con cada ingreso de personal envía esta capacitación de la política específicamente a las personas nuevas a las que ingresaron y a todas las que no hicieron la capacitación todavía. Entonces, de esa forma se va barriendo y se va alcanzando mayor adhesión.

Nunca se logra el 100%, pero se las va repitiendo en las capacitaciones hasta que se logra la mayor aproximación, no solo de la política, sino de todas las capacitaciones que se dictan: contraseñas más seguras, protocolo de protección de datos personales. Hay un montón de capacitaciones que se las hace de esa forma

Recién me nombraste que usan una herramienta para gestionar todas las capacitaciones “SmartFense”. Contame un poco acerca de las funcionalidades ¿Qué es lo que se maneja por esa herramienta?

Esta herramienta tiene distintos módulos. Se puede capacitar de distintas formas, por ejemplo, con módulos interactivos. Los módulos interactivos son pequeñas capacitaciones sobre un tema específico. La herramienta te proporciona muchas capacitaciones de esos temas y también te da la posibilidad de que armes tu propia capacitación. Por ejemplo, el protocolo de protección de datos personales ha surgido del sector de ética y compliance, entonces al ser algo muy específico, tuvo que ser desarrollado el contenido dentro de la empresa. Por lo tanto, pueden ser con contenido personalizado o como viene la herramienta.

Otra funcionalidad de la herramienta es el phishing, el ransomware te da también opciones. Te da phishing hechos para que los cambies. Lo que le cambiamos generalmente es el logo de la empresa o alguna palabra o personalizamos el sector. Detalles mínimos pero que personalizan la capacitación.

También hay newsletter que las usamos sobre algún tema específico, para variar, hay videojuegos que vamos a usar ahora por primera vez en la jornada de seguridad de la información. Vamos a hacer que las gentes se van ganando insignias en función de las capacitaciones que van realizando.

Dentro de la empresa estamos divididos en administraciones y gerencias. Entonces los usuarios van acumulando esas insignias, que son como premios y eso va a impactar directamente en el control de gestión. Todos los meses se hacen reuniones de gestión donde hay indicadores referidos a lo que es el negocio, facturación, cobranza, pérdida de energía y ahí incorporamos unos ítems que es de “seguridad de la información”, donde se van acumulando todas las insignias que van ganando las empresas por sector y eso se traduce en un color rojo, amarillo o verde, para medir la adhesión en las capacitaciones de cada uno de los usuarios.

Y esta herramienta ¿La usan desde siempre? ¿Se ha implementado ahora? ¿Usan otra herramienta?

No hace. Será que la tenemos hace tres años más o menos y antes era presencial. Todas las capacitaciones.

¿Métricas para evaluar los programas de capacitación? ¿cuáles son, para que las utilizan?

Recién están iniciando con el tema de las métricas, lo único implementado hasta ahora son la cantidad de horas de capacitación por gerencia, lo miden a través de las horas acumuladas o insignias obtenidas a través de la herramienta SmartFense, eso luego se utiliza para un tablero que se realiza en las reuniones mensuales de control de gestión de la organización, y se traduce en colores como un semáforo, según la cantidad de horas hombres realizadas.

¿Qué se hace con esas métricas?

Se busca explicar el porqué el motivo del color del indicador ante gerencia general, son indicadores para poder mejorar la cantidad de horas de capacitación

¿Se realizan planes de acción?

No se realizan planes de acción concretos, sino que se discute en la reunión de control de gestión y como a las personas no les gusta que este en rojo o en amarillo se esfuerzan para llegar a ese verde, los planes de acción es el mensaje de los jefes para su personal a cargo diciendo que realicen las capacitaciones, hay muchas capacitaciones disponibles tienen la forma de hacerlo.

¿Se considera que en la empresa existe una cultura de concientización?

No podemos decir que todavía hay una cultura, se está trabajando hace muchos años para tratar de cambiar hábitos, pero se trata de implementar la cultura porque hay contraseñas seguras, políticas de escritorios limpios, se trabaja en la cultura porque hay capacitaciones también

¿Qué reportes brinda la herramienta de capacitación? ¿Brinda algún tipo de educación para los usuarios?

La herramienta de capacitación te da reportes de auditoría, por ejemplo, la capacitación a cuantos usuarios fue enviada, cuantos la realizaron, si se trata de un phishing o un ransomware también te brinda la información, a cuantas fue enviada, cuantos abrieron ese correo y quienes no, quienes abrieron ese adjunto con el mail, cuando sucede eso el mail creado por la herramienta te lleva a lo que llama un momento educativo, en la pantalla se te abre un mensaje que dice que este email fue enviado por seguridad de la información y te brinda tips para que uno no vuelva a caer en estos adjuntos, la herramienta también se brinda la posibilidad de quienes abrieron este adjunto se les envíe una nueva capacitación.

Sobre todo tipo de capacitaciones brinda estadísticas, por ejemplo, cantidad de personas enviadas, cantidad de personas realizadas, entre otros.