Diseño de un marco de buenas prácticas para la prevención de ataques de phishing en la empresa TXOOL

Andrés Camilo Medina, Jhonatan Heli Pedraza Muñoz, Angie Paola Rivera Alba, Diego Alejandro Rojas Rincón, Valentina Solano Gutiérrez

Especialización seguridad informática, Fundación Universitaria Compensar

Propuesta de Consultoría

Ing. María Fernanda Montero Molina

15 de noviembre 2024

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Diseño de un marco de buenas prácticas para la prevención de ataques de phishing en la empresa TXOOL

Andrés Camilo Medina
Jhonatan Heli Pedraza Muñoz
Angie Paola Rivera Alba
Diego Alejandro Rojas Rincón
Valentina Solano Gutiérrez

Trabajo de grado presentado como requisito parcial para optar al título de:
Especialista en seguridad de la información

Director (a):

Ing. María Fernanda Montero Molina

Fundación Universitaria Compensar

Facultad de Ingeniería, Especialización en Seguridad Informática

Bogotá, Colombia

15 de noviembre 2024

Resumen

El objetivo de este proyecto se centra en diseñar un marco de buenas prácticas basado en la norma ISO 27001:2022 para la gestión efectiva de ataques de phishing que se puedan presentar a la empresa Txool. Para lograrlo, inicialmente se decidió analizar el nivel de madurez tecnológico de la empresa, con base a ello se diseñó el marco de buenas prácticas enfocado en la prevención de ataques de phishing, se validó el marco de buenas prácticas para realizar la presentación a Txool y se concluyó a través de un feedback por parte del gerente de IT de la compañía para lograr enfocarlo con las necesidades que presentaron. Cabe resaltar que este marco de buenas prácticas no incluye la aplicación práctica de las propuestas de mejoras y se excluyen otros tipos de ciberataque distintos al phishing.

Palabras clave: Phishing, ISO 27001, Smishing, Seguridad informática, Vishing.

Abstrac

The objective of this project is to design a set of best practices based on the ISO 27001:2022 standard for the effective management of phishing attacks that may affect the company Txool. To achieve this, the first step was to analyze the company's technological maturity level, based on which a best practices framework focused on phishing attack prevention was designed. The framework was then validated for the presentation to Txool, and the process concluded with feedback from the company's IT manager to better align it with the needs they identified. It is important to note that these best practices framework does not include the practical implementation of the proposed improvements and excludes other types of cyberattacks that are not related to phishing.

Keywords: Phishing, ISO 27001, Smishing, Computer security, Vishing.

Contenido

PÁG.

RESUMEN **5**

ABSTRAC **5**

INTRODUCCIÓN **7**

ANTECEDENTES Y JUSTIFICACIÓN 7
FORMULACIÓN DE PROBLEMA 8
OBJETIVO GENERAL 8
Objetivos Específicos *8*
ALCANCES Y LIMITACIONES 8

1. MARCO TEÓRICO **9**

1.1 CONCEPTOS BÁSICOS 9
1.1.1 Phishing *9*
1.1.2 Tipos de phishing *9*
1.1.3 Buenas prácticas *10*
1.1.4 Seguridad de la Información *10*

2. MARCO REGULATORIO **11**

3. MARCO METODOLÓGICO **11**

3.1 EVALUACIÓN INICIAL Y ANÁLISIS DE BRECHAS 11
3.1.1 Revisión de Antecedentes de la Empresa respecto a los Ataques *12*
3.1.2 Evaluación de Procesos, Herramientas y Tecnologías Actuales en Conformidad con la Norma ISO 27001:2022 ..... *12*
3.1.3 Identificación de brechas y riesgos donde Txool no Cumple con los controles de la norma ISO 27001:2022 ..... *13*
3.2 DISEÑO DE BUENAS PRACTICAS 14
3.3 PRESENTACIÓN Y ENTREGA DEL MARCO DE BUENAS PRACTICAS 17

4. RESULTADOS **18**

5. CONCLUSIONES **19**

6. RECOMENDACIONES **19**

7. REFERENCIAS **21**

8. ANEXOS **22**

Introducción

En Colombia el phishing se ha convertido en una de las mayores amenazas informáticas para organizaciones de todos los tamaños. Este tipo de ataque, que engaña a los usuarios para que revelen información sensible, ha crecido exponencialmente en los últimos años, afectando diversos sectores y resaltando la necesidad urgente de fortalecer la seguridad de la información en todas las organizaciones.

Txool, una empresa en crecimiento dedicada a la consultoría ha reconocido esta amenaza y la necesidad de actuar. Debido a la falta de medidas de seguridad tecnológica adecuadas, Txool ha identificado una brecha en la gestión respecto al phishing entre sus empleados, lo que representa una vulnerabilidad. Este proyecto busca cerrar esa brecha mediante el diseño de un marco de buenas prácticas basado en la norma ISO 27001:2022 para la seguridad de la información, logrando fortalecer y apoyar su misión de optimizar los procesos empresariales de sus clientes, garantizando un entorno de trabajo seguro.

Antecedentes y Justificación

Txool es una empresa de consultoría cuyos servicios ofrecen la optimización de procesos a sus clientes, mediante soluciones que apoyan la eficiencia operativa. No obstante, a pesar de su encuadre en la seguridad informática aplicativa, se ha identificado una debilidad con respecto a la gestión y prevención interna sobre amenazas cibernéticas entre su personal, especialmente en lo que respecta a ataques de phishing.

En 2023, tras migrar al servicio de correo electrónico a Microsoft, los empleados han recibido múltiples correos malintencionados, de los cuales algunos fueron víctimas, esto debido a la falta de procedimientos y controles adecuados. Esta vulnerabilidad ha expuesto a la empresa a riesgos que podrían comprometer sus datos y la confianza de sus clientes. Ante el creciente avance de estas amenazas, se ha vuelto crucial para Txool mejorar sus prácticas y controles con el fin de proteger sus activos y los de sus clientes, de tal forma, este proyecto busca cerrar la brecha en la capacidad de acción que presenta Txool frente a la gestión y prevención de ataques de phishing, ofreciendo un enfoque práctico adaptado a las necesidades del sector por medio del diseño de un de un marco de buenas prácticas basado en la norma ISO 27001:2022.

Formulación de problema

La compañía Txool actualmente no cuenta con herramientas de software que puedan ayudar a filtrar y bloquear correos electrónicos que contengan phishing, de igual manera, tampoco cuenta con una conciencia por parte de los empleados respecto a cómo evitar los ataques de phishing. Dentro de Txool se evidenció que estos ataques se volvieron constantes, hasta el punto en que algunos empleados reportaron incidentes vía email o por mensaje directo al área de IT, mientras que otros fueron víctimas de estos ataques, de forma que los atacantes han podido filtrar información sensible de compañía o datos confidenciales de sus clientes, es por ello que se platea la siguiente pregunta:
¿Cómo puede Txool mejorar la concientización y la capacidad de sus empleados para identificar y gestionar amenazas de phishing, con el fin de reducir el riesgo de ciberataques fortaleciendo la seguridad de la información en la empresa?

Objetivo General

Diseñar un marco de buenas prácticas basado en la norma ISO 27001:2022, que proporcione a Txool una guía estructurada para la gestión efectiva de ataques de phishing.

Objetivos Específicos

- Analizar el nivel de madurez tecnológico de Txool con respecto la identificación, gestión y prevención de ataques de phishing
- Diseñar un marco de buenas prácticas basado en la norma ISO 27001:2022 para la prevención y gestión de ataques de phishing.
- Validar el marco de buenas prácticas para la presentación y verificación con el equipo interno de Txool.

Alcances y Limitaciones

El proyecto se centra en el análisis de políticas y procedimientos establecidos por la empresa para la gestión y prevención del phishing que aplica sobre su población, siendo esta un total aproximado de 80 empleados, así mismo, se consideran modelos y marcos metodológicos relevantes, como la norma ISO 27001:2022 para gestionar y prevenir el phishing. El proyecto cuenta con apoyo institucional del equipo de asesoramiento y

utiliza datos proporcionados por Txool. Sin embargo, este estudio también presenta limitaciones, dado que no incluye la aplicación práctica de las propuestas de mejora, y adicional se excluyen otros tipos de ciberataques enfocándose únicamente en el phishing. El proyecto está limitado en términos de tiempo, ya que se presenta en noviembre como un proyecto de grado, adicionalmente, no cuenta con un presupuesto fijo, lo que restringe la disponibilidad de recursos económicos. Además, el acceso a datos confidenciales está limitado, lo que puede afectar la profundidad del análisis en algunos aspectos del estudio.

1. Marco teórico

La creciente amenaza de ataques de phishing a nivel global resalta la importancia de adoptar medidas de protección consistentes, en este capítulo se presenta la seguridad de la información mediante conceptos esenciales tomando como referencia las recomendaciones de entidades financieras nacionales.

1.1 Conceptos básicos

1.1.1 Phishing

De acuerdo con García (2021), la palabra phishing que está relacionada la palabra inglesa "fishing" o "pesca" en español, este hace referencia a la tarea de ejecutar una trampa o engañar a usuarios que navegan por Internet, lo que lleva a pensar que este acto cibernético se puede definir en la expresión coloquial "pescar insospechado". En otras palabras, el phishing es el acto descuidado de pescar incautos. (p. 22)

La Organización Internacional de Policía (INTERPOL) en su portal web oficial, define el phishing como un tipo de fraude de ingeniería social donde los ciberdelincuentes engañan y manipulan a las víctimas para que proporcionen de manera directa o indirecta información confidencial (datos bancarios, así como a datos personales, contraseñas, correos electrónicos, etc).

1.1.2 Tipos de phishing

Con base a lo escrito por Herrera (2021), existen varios tipos de phishing y cada uno con su propia forma de fraude. La mayoría de estos engaños se pueden prevenir utilizando un poco de sentido común, ya que nada se obtiene sin costo alguno. No se debe confiar en correos electrónicos que prometan acceso rápido y fácil a grandes sumas de dinero,

ni en aquellos que soliciten datos personales o contribuciones monetarias. Lo más recomendable es ignorar tales mensajes para evitar problemas. En total, se pueden identificar principalmente cinco tipos diferentes de phishing que son: Cartas Nigerianas, Estafa Piramidal, Hoax, Smishing y Vishing.

1.1.3 Buenas prácticas

Para prevenir ataques de phishing, es viable tener en cuenta las recomendaciones del escrito de Rincón (2023), estas son: Verificar los enlaces en correos-mensajes antes de hacer clic y no compartir información confidencial sin confirmar la autenticidad del remitente, mantener el navegador y programas actualizados, y asegurarse de que las páginas web empiecen con HTTPS y tengan un candado en la barra de direcciones. Utiliza extensiones anti-phishing como Windows Defender Browser Protection y busca errores gramaticales o solicitudes urgentes en mensajes sospechosos. Escribe las URL manualmente y usa marcadores para acceder a sitios seguros, evitando introducir información en ventanas emergentes sospechosas. Recuerda que el phishing también puede ocurrir en redes sociales y aplicaciones, así que comparte información con precaución.

También es útil seguir las directrices de una entidad bancaria como lo es Bancolombia, que recomienda: Acceder siempre a la Sucursal Virtual Personas a través de su página web oficial, escribiendo la dirección directamente en la barra del navegador; no usar enlaces recibidos por correo ni acceder desde sitios públicos como cibercafés. Bancolombia nunca solicitará datos personales o información de cuentas por correo electrónico. No compartir información confidencial durante llamadas telefónicas. Mantener la computadora actualizada con herramientas de seguridad y verifica que las páginas de compras en línea sean seguras.

1.1.4 Seguridad de la Información

Según Kaspersky (2019), La seguridad de la información se refiere a las prácticas, políticas y tecnologías diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos. Su objetivo es garantizar que la información solo sea accesible para usuarios autorizados, que no se modifique sin permiso y que esté disponible cuando se necesite. La amenaza creciente a la información en Latinoamérica

alcanza un 60%, lo que subraya la necesidad de que los usuarios de sistemas de información adopten medidas para proteger este recurso vital. Las amenazas actuales incluyen fraudes informáticos, espionaje, sabotaje, vandalismo, desastres naturales y la falta de precaución por parte de los usuarios. La relevancia de la seguridad de la información ha aumentado con el tiempo debido al incremento en el uso de sistemas de información por parte de las organizaciones, lo que hace que estos sistemas sean objetivos atractivos para los atacantes. Dado que se maneja una cantidad cada vez mayor de información, las consecuencias de su sustracción se vuelven más graves. Por lo tanto, el número de ataques crece en paralelo con el uso y diversificación de los sistemas, ya que los atacantes encuentran nuevas formas de eludir las medidas de seguridad.

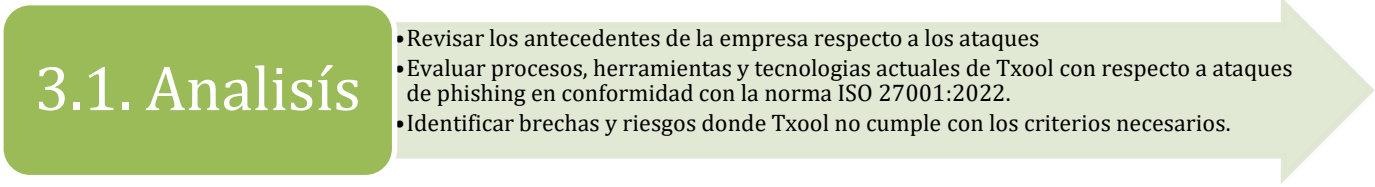
2. Marco Regulatorio

De acuerdo con el análisis de los antecedentes de la compañía, el marco de buenas prácticas infiere de la información obtenida con base en el estándar de la ISO/IEC 27001:2022, puesto que esta norma ha proporcionado una serie de controles y directrices que las organizaciones deben seguir para la gestión de seguridad de la información y poder mitigar los incidentes de seguridad informática y ciberseguridad respecto al phishing permitiendo diseñar un marco de buenas prácticas con el fin de que la compañía pueda prevenir y mitigar incidencias de seguridad de la información respecto al phishing en conformidad con las regulaciones pertinentes tanto nacionales como internacionales.

3. Marco metodológico

Para el diseño del marco de buenas prácticas enfocado a la gestión y prevención del phishing en la empresa Txool, se contemplaron tres fases importantes, las cuales corresponden a los objetivos específicos propuestos:

3.1 Evaluación Inicial y Análisis de Brechas



3.1.1 Revisión de Antecedentes de la Empresa respecto a los Ataques

En esta fase se analizó el historial de Txool en relación con los ataques de phishing. Tras la migración al servicio de correo electrónico de Microsoft en 2023, la empresa experimentó un aumento en correos maliciosos en los cuales suplantaban la identidad del CEO, pese a que la empresa no posee ningún software o portal para el reporte y seguimiento de incidentes, se logró identificar mediante historial de correo electrónico un grupo considerable de empleados que fueron víctimas de estos ataques debido a la falta de concientización y medidas de seguridad adecuadas. Este hecho evidenció la necesidad urgente de abordar el problema para proteger los datos de la empresa y mantener la confianza de los clientes.

3.1.2 Evaluación de Procesos, Herramientas y Tecnologías Actuales en Conformidad con la Norma ISO 27001:2022

Se llevó a cabo un análisis detallado de los procesos y herramientas actuales de Txool con respecto a la protección frente a ataques de phishing, utilizando 18 controles de la norma ISO 27001:2022 como referencia. En esta evaluación, se centró en los siguientes aspectos:

- **Procesos y Políticas**: Se evaluaron las conductas de seguridad de la información, evidenciando la ausencia de políticas específicas para abordar el phishing y la falta de procedimientos claros para la prevención y gestión de estos ataques.
- **Herramientas Tecnológicas**: Se revisaron las soluciones actuales, como los filtros de correo, destacando que no están configuradas para contrarrestar técnicas de phishing avanzadas y que la falta de un dominio propio dificulta la actualización regular de las medidas de seguridad como actualizaciones de sistema o restricciones en la red.
- **Capacitación y Concientización**: Se analizó el nivel de preparación del personal en ciberseguridad, encontrando una ausencia de programas formales de formación y concientización en la detección y gestión de intentos de phishing.

3.1.3 Identificación de brechas y riesgos donde Txool no Cumple con los controles de la norma ISO 27001:2022

En la Tabla 1 se resume el estado de cumplimiento de los 18 controles relevantes de la ISO 27001:2022, destacando las áreas que requieren mejoras significativas respecto a la prevención de phishing.

Tabla 1. Resultado de evaluación sobre 18 controles ISO 27001:2022 en Txool

Control	Tipo	Estado	Implementación y Hallazgos
5.01	Políticas de seguridad de la información	Inexistente	No existe una política formal, y no está claramente definida ni publicada.
5.02	Roles y responsabilidades de seguridad de la información	Inicial	Solo una persona se encarga de la prevención y respuesta a phishing, y no hay una comunicación clara entre el personal.
5.04	Responsabilidades de gestión	Inexistente	No hay acciones de seguimiento o monitoreo por parte de la gerencia.
5.07	Inteligencia de amenazas	Inicial	Aunque los usuarios reportan desde Outlook, no hay un análisis formal de tácticas o amenazas emergentes.
5.12	Clasificación de la información	Limitado	Se utilizan herramientas de Microsoft para restringir accesos, pero no hay una clasificación formal de contraseñas u otros datos sensibles.
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Inicial	Solo una persona gestiona los incidentes, y no hay roles ni planes de acción claramente definidos para otros empleados.
5.25	Evaluación y decisión sobre eventos de seguridad de la información	Limitado	Se apoya en herramientas de Microsoft para la revisión, pero no hay criterios de evaluación definidos.
5.26	Respuesta a incidentes de seguridad de la información	Inicial	No existen procedimientos documentados ni una respuesta organizada más allá del bloqueo de remitentes.
5.27	Aprender de los incidentes de seguridad de la información	Inexistente	No se documenta ni se aprovecha la información de incidentes anteriores.
5.28	Recolección de evidencia	Inexistente	No hay un procedimiento formal para la recolección ni preservación de evidencia más allá del historial en correo electrónico.
5.35	Revisión independiente de la seguridad de la información	Definido	Se revisa regularmente, aunque las revisiones son muy básicas y no están avaladas por un estándar externo.
5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	Inexistente	No hay auditorías internas ni políticas formales contra el phishing.
6.02	Términos y condiciones de empleo	Inicial	No se incluyen responsabilidades específicas en los contratos de trabajo, únicamente se menciona en el onboarding.
6.03	Concientización, educación y capacitación en seguridad de la información	Inicial	Las capacitaciones se dan solo después de incidentes significativos y no hay un programa establecido.
6.04	Proceso disciplinario	Inexistente	No hay un proceso disciplinario formal para tratar incidentes de phishing.
6.08	Informes de eventos de seguridad de la información	Limitado	Existen mecanismos de reporte, pero no se asegura la oportunidad ni el uso de canales adecuados.
8.12	Prevención de fuga de datos	Inexistente	No hay medidas formales para la prevención de fuga de datos más allá de las que ofrece Microsoft.
8.16	Actividades de seguimiento	Inicial	Se revisan alertas y se bloquean remitentes, pero no hay un seguimiento continuo o estructurado.

En la Ilustración 1 se muestra la proporción de controles que no cumplen con los requisitos establecidos en la norma. Este análisis brindó una visión clara de los puntos débiles en el sistema de gestión de seguridad de la información de la empresa y apoya a la toma de decisión sobre cuales priorizar.

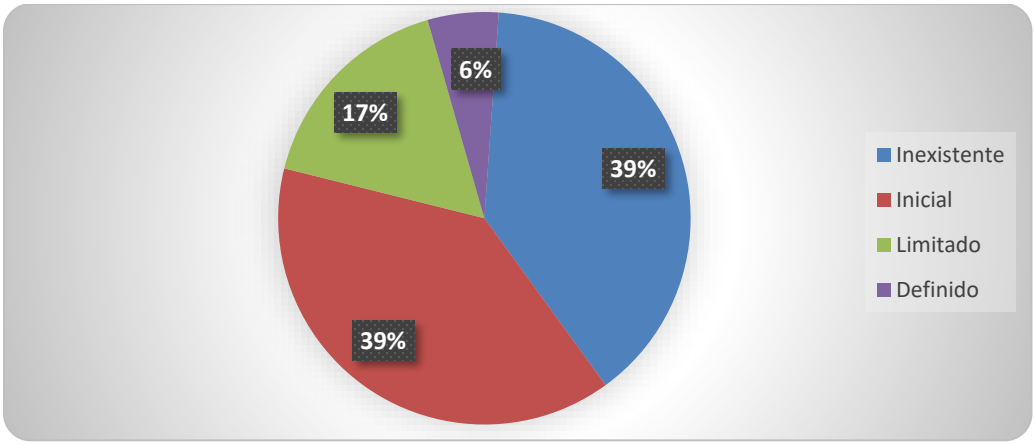


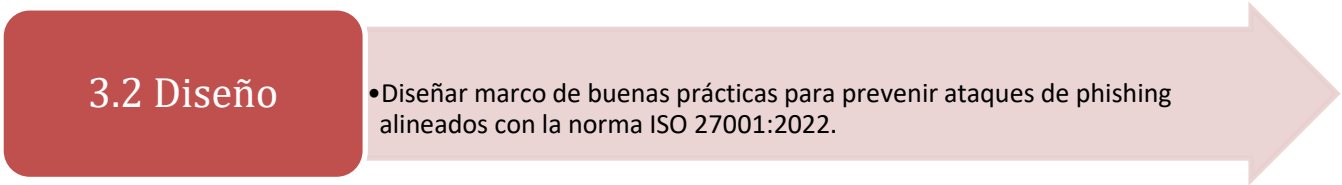
Ilustración 1. Estado de Implementación Controles Contra Phishing ISO27001:2022 - Txool

Nota: elaboración propia

Como resultado de la evaluación sobre el estado de implementación de controles basados en la norma ISO 27001:2022 se logró identificar que la empresa posee carencias para gestionar y prevenir vulnerabilidades con relación al phishing resaltando los siguientes aspectos de mejora:

- **Falta de Políticas Específicas sobre Phishing**: La ausencia de directrices claras aumenta la vulnerabilidad ante estos ataques.
- **Deficiencias en las Herramientas de Seguridad**: Las soluciones actuales no son suficientes para detectar ataques sofisticados.
- **Ausencia de Programas de Capacitación**: Sin formación adecuada, los empleados no están preparados para enfrentar amenazas de phishing.
- **No Conformidad con la ISO 27001:2022**: Txool no cumple con controles esenciales de la Norma.

3.2 Diseño de buenas practicas



Se diseñó una serie de recomendaciones alineadas con los controles de la norma ISO 27001:2022, con el fin de mejorar la capacidad de Txool para prevenir ataques de phishing. Estas recomendaciones buscan cumplir con los requisitos de seguridad de la norma, abarcando la optimización de procesos, el fortalecimiento de las herramientas tecnológicas, y el incremento de la capacitación del personal.

En la Tabla 2 se detalla la relación de cada control de la ISO 27001:2022 con las propuestas de mejora, proporcionando un marco claro de acciones correctivas y preventivas.

Tabla 2. Recomendaciones de implementación sobre controles ISO 27001:2022 en Txool

Control	Tipo	Acción de mejora
5.01	Políticas de seguridad de la información	Se recomienda definir la política de seguridad de la información que abarque el ciclo de vida de los activos de información de la empresa. Definiendo y desarrollando políticas específicas o de nivel II, teniendo en cuenta: protección de la información sensible, gestión de incidentes de seguridad y reglas para uso de los sistemas informáticos, una vez creada la política debe ser presentada a la alta dirección para su debida revisión, aprobación y compromiso de su implementación y cumplimiento. La política debe ser comunicada de manera eficaz a todos sus empleados y para finalizar se debe revisar periódicamente las políticas ante cambios significativos de la empresa y/o algún requisito legal. En el **Anexo 1** se detalla el plan de mejora para este control.
5.02	Roles y responsabilidades de seguridad de la información	Se recomienda identificar de los roles existentes en la empresa y determinar responsabilidades de cada rol en relación con la seguridad de la información. En caso de ser necesario definir y asignar nuevos roles designando a las personas con actividades de seguridad como equipos de respuesta a eventos o incidentes y promoción de cultura de seguridad. Posteriormente se deben documentar los procedimientos para cada actividad relacionada con seguridad, Así mismo los roles y las responsabilidades de los empleados que se definan deben ser comunicadas a todos los empleados de la empresa y para finalizar; revisar periódicamente la estructura de roles y responsabilidades y en caso de ser necesario, realizar los ajustes pertinentes frente a cambios organizativos.
5.04	Responsabilidades de gestión	Se recomienda hacer un análisis de los procesos de negocio identificando aquellos que involucren el manejo de información posteriormente, y la creación de flujogramas que los relacionen entre ellos. También se recomienda definir una matriz que relacione las responsabilidades definidas de cada rol y que no se interpongan entre ellas, posteriormente se recomienda documentar los procesos que detallen los pasos para realizar cada una de las tareas y para finalizar, se recomienda revisar periódicamente si las responsabilidades siguen siendo adecuadas, en caso de ser necesario, realizar los ajustes pertinentes frente a cambios tecnológicos y organizativos.
5.07	Inteligencia de amenazas	Se recomienda establecer procesos de recolección de información sobre noticias de ciberataques vulnerabilidades, informes de seguridad teniendo presente las diferentes fuentes de información, canales y frecuencia, analizando la información recolectada teniendo criterios de clasificación priorización y evaluación, con el fin de identificar tendencias de amenazas. Se recomienda manejar la información para implementar evaluaciones de riesgo, aplicar controles para mitigar amenazas, planificación de respuesta a eventos o incidentes y crear campañas o comunicados para los empleados de la empresa.
5.12	Clasificación de la información	Se recomienda establecer una política de seguridad de clasificación de la información y que esta debe ser informada a todos los empleados. Dicha política se puede implementar bajo un esquema de clasificación de confidencialidad enfocados en la disponibilidad, integridad y confidencialidad de la información, la cual se puede clasificar de la siguiente manera según su nivel de importancia: La divulgación que no causa daño - La divulgación que causa un daño reputacional menor o un impacto operativo menor - La divulgación que tiene un impacto significativo a corto plazo en las operaciones - La divulgación que tiene un impacto grave a largo plazo o pone en riesgo la supervivencia de la empresa.
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Se recomienda preparar y planificar una gestión acorde para los incidentes de seguridad de la información que se puedan presentar, para ello deben definir, establecer y comunicar procesos, funciones y responsabilidades de gestión para estos incidentes; de esta manera se podrá garantizar una respuesta mucho más rápida, eficaz, coherente y ordenada. Se recomienda que, de igual manera, estos casos sean documentados y salvaguardados de manera segura para tenerlos en cuenta en caso de que se presente algún incidente similar a futuro.
5.25	Evaluación y decisión sobre eventos de seguridad de la información	Se recomienda evaluar los eventos de seguridad de la información y decidir si se clasificaran como incidentes de seguridad, acordar un esquema de categorización y prioridad de un incidente, luego el punto de contacto deberá evaluar cada evento de seguridad basado en el esquema. El personal definido de coordinar y responder ante estos incidentes en la empresa deberá tomar la evaluación y tomar una decisión sobre los eventos de seguridad de información y los resultados deberán ser documentados a detalle para fines de futura referencia y revisión. Se da ampliación del plan de mejora en el

Control	Tipo	Acción de mejora

Anexo 2

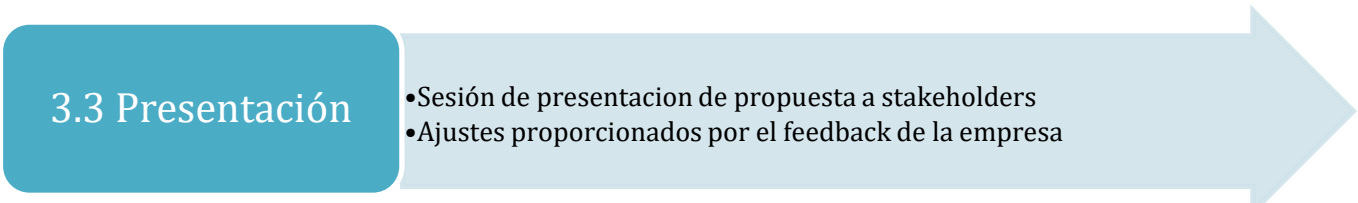
5.26	Respuesta a incidentes de seguridad de la información	Se recomienda crear un protocolo de respuesta si las consecuencias del incidente pueden extenderse, para ello se recomienda recopilar todo tipo de evidencia tan pronto como sea posible después de la ocurrencia, escalar según sea necesario y a las áreas encargadas, garantizar que todas las actividades de respuesta involucradas se registren correctamente para su posterior análisis, comunicar la existencia del incidente o cualquier detalle relevante del mismo a todas las partes interesadas internas y externas pertinentes, coordinar todas las partes para lograr una mejora de respuesta y minimizar consecuencias y una vez finalizado el incidente, deberá cerrarse y registrarse formalmente. También se recomienda realizar análisis forenses de seguridad de la información, según se requiera.
5.27	Aprender de los incidentes de seguridad de la información	Se recomienda establecer un proceso continuo de gestión de incidentes, en el cual se realice la identificación y registro de todos los intentos de phishing al igual se deberá realizar análisis post- incidentes para determinar cuál es la causa y la raíz esto para poder ajustar las políticas de seguridad. De acuerdo con los incidentes se recomienda adecuar capacitaciones que concienticen sobre el phishing en la empresa. En el **Anexo 3 s**e detalla el plan de mejora para este control.
5.28	Recolección de evidencia	Se recomienda establecer un proceso fuerte de monitoreo y de seguimiento en seguridad de la información donde se identifiquen los ataques de phishing, donde se implementen herramientas de detención y una serie de auditorías periódicas esto con el fin de tener evidencias de los incidentes de phishing, donde no se permita la manipulación de otras personas que puedan alterar las evidencias.
5.35	Revisión independiente de la seguridad de la información	Se recomienda implementar una serie de revisiones periódicas de sus prácticas de seguridad en referencia a la gestión, detección y prevención de phishing. Por lo cual se recomienda tener dos Auditores uno externo y uno interno que permitan dar un alcance a la política y a los

Control	Tipo	Acción de mejora
		procedimientos respecto a los hallazgos que puedan existir respecto del phishing que sean imparciales en la toma de los muestreos.
5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	Se recomienda realizar un plan de seguimiento a las políticas específicas, las reglas y los estándares establecidos respecto al phishing, se recomienda tener revisiones ya sean periódicas o mensuales para detectar el incumplimiento de estas. Por otra parte, también se recomienda implementar una serie de acciones que lleven a la corrección de incumplimiento tomando en cuenta la identificación de la deficiencia y la debilidad.
6.02	Términos y condiciones de empleo	Se recomienda varias acciones clave para mejorar la seguridad de los datos dentro de la empresa. Como primer paso, se llevar a cabo una revisión exhaustiva de los contratos existentes para identificar y complementar cláusulas que definan claramente las obligaciones de seguridad de los datos. Definir de forma precisa los roles y el establecimiento de obligaciones de cumplimiento contractual. Además, se recomienda implementar programas de capacitación adecuados para garantizar que todos los empleados comprendan sus responsabilidades de seguridad. Por último, se recomienda establecer revisiones periódicas de los contratos y las políticas para garantizar que se mantengan actualizados y sean eficaces ante la evolución de las amenazas a la seguridad.
6.03	Concientización, educación y capacitación en seguridad de la información	Se recomienda evaluar las necesidades de capacitación en seguridad de la información en función del rol de cada empleado. Esto incluye el desarrollo de programas de capacitación sobre políticas de seguridad, manejo de información sensible y prevención de incidentes. Se recomienda realizar sesiones periódicas de desarrollo profesional para mantener a los empleados actualizados sobre los cambios y las mejores prácticas, y se recomienda realizar evaluaciones para medir la eficacia de la capacitación. Finalmente, se recomienda documentar toda la capacitación y obtener las firmas de los empleados como prueba de su participación.
6.04	Proceso disciplinario	Se recomienda establecer un proceso disciplinario formal y claro que detalle las acciones tomadas por violaciones a las políticas de seguridad de la información. Este proceso debe comunicarse de manera efectiva a todos los empleados y partes interesadas a través de reuniones y documentos formales. Además, se recomienda implementar un sistema para registrar y revisar las infracciones para garantizar que se realice un seguimiento adecuado de cada incidente. Se recomienda capacitar a los gerentes y supervisores para que apliquen este proceso de manera justa y consistente es esencial para mantener la integridad del sistema. Finalmente, se recomienda revisar periódicamente el proceso para garantizar que sea eficiente y siga las mejores prácticas de seguridad de la información.
6.08	Informes de eventos de seguridad de la información	Se sugiere a la empresa implementar un mecanismo eficaz y accesible para que los empleados informen sobre incidentes de seguridad de la información observados o sospechados. Se recomienda que este sistema asegure una comunicación oportuna a través de canales adecuados, permitiendo que todos los empleados conozcan los procedimientos y la importancia de reportar incidentes con prontitud. Se recomienda desarrollar una cultura de transparencia y responsabilidad ayudará a aumentar la seguridad general de la información y minimizar los riesgos asociados con ataques como el phishing. En el **Anexo 4** se detalla el plan de mejora para este control.
8.12	Prevención de fuga de datos	Se aconseja establecer acciones de prevención de infracciones de datos en todos los sistemas, redes y aparatos que manejan, resguardan o envían datos sensibles. Esto debería abarcar evaluaciones de riesgos para detectar vulnerabilidades, puesta en marcha de controles técnicos como el cifrado y filtrado de contenido, y seguimiento constante de acciones atípicas. Además, es aconsejable que los trabajadores sean formados en políticas de salvaguarda de datos y mejores prácticas para disminuir el peligro de infracciones de datos. Finalmente, se aconseja llevar a cabo revisiones regulares para evaluar y renovar las medidas de seguridad con el fin de asegurar su efectividad y adaptabilidad frente a nuevas amenazas.
8.16	Actividades de seguimiento	Se recomienda implementar sistemas de monitoreo para identificar comportamientos anormales en redes, sistemas y aplicaciones. Además, se recomienda establecer procedimientos claros de seguimiento a estos incidentes, asegurando una respuesta adecuada y oportuna que mejore la protección de la confidencialidad, integridad y disponibilidad de la información.

Concluyendo la fase 2, se pudo evidenciar como Txool ante la carencia de cumplimiento de múltiples controles de la norma fue objeto de diversas propuestas de mejora por parte del equipo del proyecto con relación a los 18 controles respectivos, siendo estas propuestas, principalmente enfocadas a la definición de políticas claras y la generación de planes de acción y concientización que permitan a la empresa prevenirse frente a la posible materialización de un riesgo de phishing, de tal forma, en los siguientes Anexos: Anexo 1,

Anexo 2, Anexo 3 y Anexo 4, se detalla el plan de mejora para los controles correspondientes.

3.3 Presentación y entrega del marco de buenas practicas



Se llevó a cabo una sesión con el gerente de tecnología de la empresa en donde se presentó a Txool los aspectos que se evaluaron, los criterios y las personas a las cuales se entrevistó, posteriormente se comunicó de forma verbal la síntesis de la evaluación

realizada en relación con los 18 controles de la norma ISO27001:2022 relevantes a vulnerabilidades de Phishing, a su vez se mostró la Ilustración 1 de forma que la gerencia pudo adquirir una visión clara de su estado actual y de las falencias que están presentando como empresa.

A continuación, se hizo mención sobre las propuestas de mejora correspondiente a los controles en no conformidad, exponiendo la Tabla 2. Recomendaciones de implementación sobre controles ISO 27001:2022 en Txool, donde se pudo contrastar el trabajo que la empresa deberá desempeñar para poder lograr un estado de cumplimiento satisfactorio.

Adicional se recibió feedback de parte de la gerencia, en donde se resaltó principalmente su preocupación por el estado actual de la empresa y se recalcó su compromiso por mejorar la seguridad de la información mostrando su interés por iniciar a la brevedad con las acciones correctivas, adicionalmente, la gerencia solicitó un ajuste mínimo a nivel de diseño sobre Ilustración 1, en el cual se ajustó el porcentaje mostrado. Finalmente se compartió con la gerencia un formulario de Teams a diligenciar con el cual se reafirmó la satisfacción de la empresa con respecto al proyecto desarrollado.
En la Tabla 3 se presentan los resultados de la reunión realizada con la empresa, al líder de gestión de tecnología en la cual se utilizó el siguiente Anexo 5- formulario satisfacción en cara a lo propuesto.

Tabla 3. Retroalimentación Txool

Ítem	**Respuesta**
Nombre completo	Luis Alejandro Cárdenas Vargas
Cargo	Líder Gestión de la Tecnología
Correo electrónico	luis.cardenas@txool.com
¿Qué tan útil considera que es el marco presentado para su empresa?	10
¿Qué tan bien se abordaron sus inquietudes o preguntas durante la presentación?	10
¿Qué tan probable es que usted considere aplicar las recomendaciones del marco presentado?	10
¿Hubo algún tema que le gustaría que se hubiera tratado con más profundidad?	No, el alcance de la sesión fue el adecuado
¿Hubo algún aspecto de la presentación que no le gustara o que considere mejorable?	No, solo hice un comentario de mejora de una tabla para una mejor interpretación. De todo lo demás estuvo correcto y acorde.

4. Resultados

Dado que la empresa no presentaba alguna evaluación o auditoria previa, se tomó la validación de resultados como un punto inicial sobre la auditoría realizada en Txool, siendo esta aplicada por medio del formato de entrevista al personal interno de tecnología, alineando las preguntas fielmente a la norma ISO 27001:2022 asegurando de esta forma el nivel confiabilidad en las respuestas brindadas por los entrevistados, aquí se pudo constatar que la empresa se encuentra en un estado no optimo en cuanto al cumplimiento de la norma ISO 27001:2022 dado que, sobre los 18 controles evaluados, existe un equivalente al 78% de controles que se encuentran en estado inexistente o inicial, esto permitió al equipo del proyecto diseñar diversas propuestas de mejora, mencionadas en la Tabla 2, abarcando principalmente la definición de políticas, mejora a las herramientas internas e implementación de planes de capacitación.

Culminando así con el diseño del marco de buenas prácticas, posteriormente se obtuvo retroalimentación por parte de la empresa, donde este mostro entusiasmo y compromiso en velar por el cumplimiento de los controles en base a las recomendaciones proporcionadas.

5. Conclusiones

- Se identifico el nivel de madurez tecnológico y se determinó la deficiencia de las herramientas internas para la detección, gestión y prevención de phishing puesto que son insuficientes e inexistentes.
- Se diseño un marco de buenas prácticas basado en la norma ISO 27001:2022 enfocado en los 18 controles del anexo A, relacionados con la prevención y gestión de ataques de phishing.
- Se validó el marco de buenas prácticas, donde se presentó ante el gerente de TI el resultado de la evaluación realizada en la empresa Txool. Aquí, se evidenció que los resultados y las mejoras propuestas corresponden a las necesidades de la organización.

6. Recomendaciones

- Desarrollar un plan de acción para el cumplimiento de los controles estándar, priorizando los controles más críticos.
- Incluir herramientas internas de detección y prevención de phishing
- Establecer políticas de seguridad específicas para prevenir el phishing y hacerlas accesibles y comunicadas a los empleados.
- Implementar un programa de formación en seguridad y prevención de phishing para todos los empleados.
- Trabajar con el equipo para validar el marco de mejores prácticas y establecer sistemas de seguimiento para garantizar su eficacia.

7. Referencias

Bancolombia. (16 de Marzo de 2022). *¿Qué es y cómo evitar el phishing?* Obtenido de https://www.bancolombia.com/centro-de-ayuda/preguntas-frecuentes/que-es-phishing-evitarlo

COLOMBIA, E. C. (enero de 2009). *Ley 1273 de 2009*. Obtenido de Ley 1273 de 2009: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

COLOMBIA, E. C. (17 de octubre de 2012). *LEY ESTATUTARIA 1581 DE 2012*. Obtenido de https://www1.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Consejo de Europa División de Ciberdelito. (Junio de 2021). *El Convenio de Budapest sobre la Ciberdelincuencia*. Obtenido de https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA. (06 de Julio de 2016). *relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.* Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

IBM. (2024). *Informe del costo de una filtración de datos 2024*. Obtenido de https://www.ibm.com/mx-es/reports/data-breach

ISO. (2022). *ISO/IEC 27001:2022.* Obtenido de https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

MentorDay. (2024). *Ciberseguridad para emprendedores.* MentorDay.

Parlamento Europeo y del Consejo. (27 de Abril de 2016). *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO*. Obtenido de REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Quintero, L. N. (26 de Febrero de 2024). *El falso mensaje a nombre de la Dian con el que pretenden estafar personas en Colombia.* Obtenido de https://www.eltiempo.com/economia/sectores/dian-falso-mensaje-con-el-que-estafan-a-personas-contribuyentes-en-colombia-858763

Sánchez, E. Y. (2021). *Delitos Contra El Patrimonio Económico, El Phishing En Colombia, Aproximación Criminológica.* Bogota: Universidad Nacional .

Universidad libre . (2024). *Crecen los ataques de phishing en Colombia*. Obtenido de https://www.unilibre.edu.co/Bogota/noticias/424-taller-declaracion-de-renta-personas-naturales#:~:text=En%20Colombia%20al%20mes%2C%20se,como%20claves%20bancarias%2C%20n%C3%BAmero%20de

8. Anexos

Anexo 1

Plan de mejora del control 5.1 política de seguridad de la información

- **Objetivo**

El objetivo principal de la política es garantizar la seguridad de los pilares de la información la confidencialidad, integridad y disponibilidad de empresa.

- **Alcance**

Esta política se aplica a toda la información de la empresa, incluyendo datos personales de clientes, empleados, procesos, contratos terceras partes propiedad intelectual, información de procesos y todo aquel que tenga vinculación alguna.

1. **Responsables**

- **Alta Dirección:** Asegura el compromiso con la seguridad de la información, proporciona los recursos necesarios y revisa periódicamente la política.
- **Departamento de seguridad de la información:** Encargados de la implementación monitoreo y cumplimiento de los controles de seguridad.
- **empleados:** Responsables de proteger la información de la empresa y reportar cualquier incidente de seguridad.

2. **Principios**

- **Confidencialidad:** La información se protegerá de la divulgación a personas no autorizadas.
- **Integridad:** La información se protegerá contra modificaciones no deseadas.
- **Disponibilidad:** La información debe ser accesible cuando sean necesarios.

3. **Controles (basados en ISO 2700)**

Se toman los controles relevantes y afines sobre las buenas prácticas para prevenir y salvaguardar la empresa de ciberataques de tipo phishing que se encuentran descritos en el marco de buenas prácticas.

6. Vigilancia y Mejora Continua Se deben realizar revisiones periódicas de la política y del SGSI para garantizar su eficacia.

7. Incumplimiento El incumplimiento de la política puede resultar en sanciones disciplinarias, legales, incluyendo el despido siempre y cuando aplique.

Anexo 2

Plan de mejora del control 5.25 Evaluación y decisión sobre eventos de seguridad de la información

- **Alcance**

Este control abarca la evaluación de los eventos de seguridad de la información y las decisiones para validar cuales de estos clasifican como incidentes de seguridad con el fin de documentarlos para mitigar riesgos similares a futuro.

- **Objetivo**

Asegurar una categorización y priorización de los eventos de seguridad de la información enfocados en phishing recomendando el siguiente paso a paso:

1. **Identificar los riesgos:** Es necesario que Txool registrar los eventos de seguridad en su totalidad y en tiempo real, entre estos eventos se deben registrar accesos no autorizados, cualquier sospecha de intrusión y cualquier vulnerabilidad que sea relevante a criterio de la empresa. Para ello se recomienda utilizar herramientas de gestión de evento (SIEM) como por ejemplo Elastic SIEM para poder recopilar datos y generar alertas con el fin de clasificar y priorizar los eventos que se van registrando.

2. **Evaluar la gravedad:** Una vez identificados los riesgos, es importante realizar una evaluación de gravedad e impacto de cada evento phishing o incluso cualquier ciberataque, como buena práctica se podría tener un apoyo con una matriz de riesgos gravedad x impacto para los eventos y poder clasificarlos por nivel de riesgo.

3. **Decidir sobre acción:** Las personas encargadas que asigne Txool deberán realizar una toma de decisiones como precaución según lo demande la situación (depende del nivel de riesgo que sea identificado a raíz de un evento que se esté presentando). Si el riesgo es significativo, se recomienda aislar sistemas, bloquear accesos, aplicar parche en caso de ser necesario mientras se escala el incidente al área pertinente para obtener un mejor análisis.
4. **Escalar el caso:** Luego de tomar la decisión y si el equipo de Txool ve necesario que el evento deba ser escalado, se recomienda tener un plan de acción ante situaciones que puedan ocurrir a futuro, para ello se

pueden implementar pruebas periódicas de simulaciones de ataques de phishing con base a los riesgos identificados (punto 1) y que sean necesarios. Esto con el fin de tener una coordinación estandarizada a los otros equipos como TI, legales e incluso relaciones públicas para tener una respuesta más efectiva y eficiente.

5. **Documentar el caso:** Es necesario que en cada incidente que se llegue a presentar en Txool se documente con fecha y hora para marcar una trazabilidad lógica a todas las decisiones y acciones de cada equipo o área que se involucró con la gestión del evento. Esta documentación se puede tomar como una guía de respuesta que pueda ayudar a prevenir incidentes similares a futuro.

6. **Mejora continua:** Para evitar que algunos casos similares a futuro tengan una gran repercusión es necesario que Txool maneje una mejora continua, esto lo puede realizar bajo un análisis post-**incidente** sobre las causas para mitigar el riesgo en las distintas áreas que se vieron comprometidas en los ataques. Esto se puede ejecutar bajo una actualización de políticas y/o controles de seguridad, junto con una capacitación al personal que considere necesario, la empresa enfocada en el riesgo de abrir correos con dominios que no son oficiales o que contengan un enlace que no se vea seguro a primera vista.

Anexo 3

Plan de mejora del control 5.27 Aprender de los incidentes de seguridad de la información respecto al phishing

- **Objetivo**

Aumentar la capacidad por parte de la empresa para aprender de aquellos incidentes de phishing, mejorando la detección, respuesta y prevención de futuros incidentes cumpliendo con el estándar de la ISO 27001/022

- **Alcance**

Esto aplica para todos los usuarios y sistemas dentro de la empresa que pueden estas involucrados en un incidente de Phishing

Dada la situación actual respecto con los incidentes de phishing dado que este control es nulo dentro de la empresa se contempla el siguiente plan de mejora:

1. **Acciones preventivas**

   - Se recomienda la programación de capacitaciones sobre seguridad enfocado en el tema de phishing mostrando estadísticas respecto a la empresa en cuanto a los casos que se han tenido dentro de esta.
   - Se recomienda la realización de campañas de phishing esto con el fin de evidenciar el aprendizaje de las capacitaciones al igual se debe realizar valoración antes y después de las capacitaciones.

2. **Acciones correctivas**

- se recomienda la creación de una política especifica respecto al aprendizaje de los incidentes.
- se recomienda la creación de una bitácora de incidentes donde se vea la fecha, el incidente y su posible solución.
- Se recomienda establecer unos filtros de correo electrónico y un sistema de detención de phishing

3. **Monitoreo**
   Realizar análisis de manera mensual de los registros de incidentes pasados para poder ver patrones o tendencias.
4. **Responsabilidad**

Crea un grupo encargado de analizar las incidencias ocurridas y también quien estará dedicado a la respuesta de los incidentes de phishing de la compañía

Crear o garantizar que el equipo de incidencias este capacitado de manera adecuada para brindar apoyo y capacitación a las demás áreas de la empresa.

5. **Recursos**

   Se recomienda utilizar herramientas como Miteru donde nos permite el bloque de páginas falsas, phishing cátcher la cual permite detectar dominios de phishing e igualmente bloquearlos o para el tema en nube esta PhishTitan que es una inteligencia artificial que detecta y bloque correos electrónicos de phishing

6. **Evolución de resultados**

   Se recomienda el manejo de KPIs para establecer cuantos incidentes han sucedido y luego de realizar las recomendaciones necesarias cuanto ha reducido en dichos casos.

7. **Documentación y registro**

   Se recomienda la documentación mensual de los incidentes esto con el fin de cumplir en las auditorias y llevar el debido control.

   Se recomienda hacerle seguimiento continuo tanto a la documentación como a la solución probable de dichos incidentes de seguridad.

Anexo 4

Plan De Mejora Control 6.08: Informes De Eventos De Seguridad De La INFORMACIÓN

1. Implementación y Hallazgos

Existen mecanismos de reporte, pero no se asegura la oportunidad ni el uso de canales adecuados.

2. Objetivo

El objetivo principal de la política es que se pueda obtener un mapeo sobre los incidentes y/o ataques de phishing que se puedan presentar.

3. Plan de acción:

1. **Implementar un sistema de notificación de incidentes**
   - Herramientas recomendadas: Implementar Jira Service Management o ServiceNow para que los empleados puedan informar incidentes de seguridad de manera rápida y eficiente.
   - Establecer un portal de informes de seguridad interno y accesible, disponible las 24 horas, los 7 días de la semana.

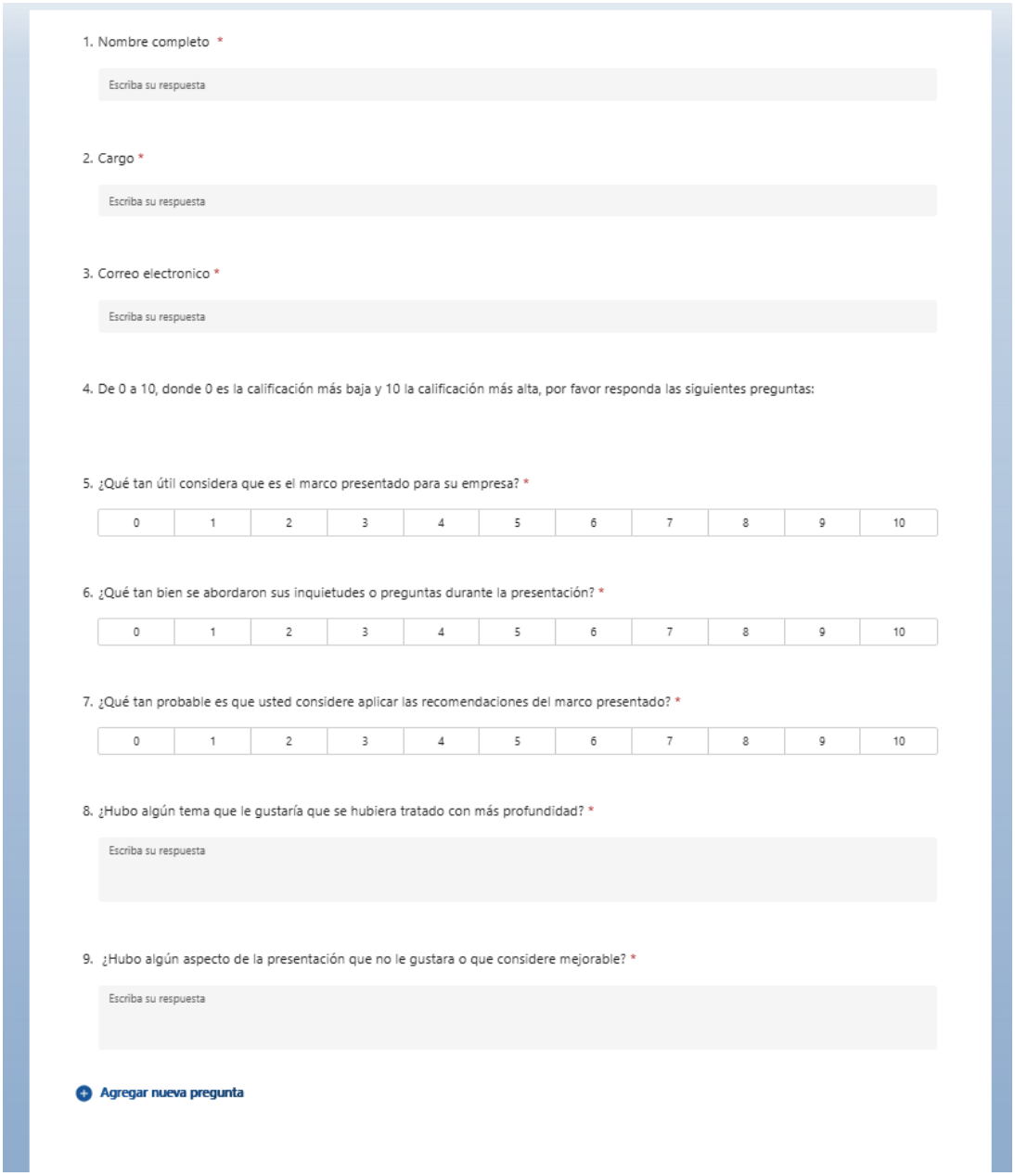
2. **Capacitación continua del personal**
   - Herramientas recomendadas: Utilizar KnowBe4 o Cofense para simulaciones y entrenamiento de phishing.
   - Organizar sesiones periódicas de concientización sobre cómo identificar y reportar incidentes de seguridad.

3. **Definir y promover canales de comunicación claros**
   - Establecer correos electrónicos y números de teléfono específicos para incidentes de seguridad, comunicando claramente cómo y cuándo utilizar estos canales.

4. **Promover una cultura de responsabilidad.**

- Crear documentación que explique la importancia de reportar incidentes con prontitud y difundirla a través de boletines internos o intranet. Monitorear y evaluar el sistema de informes.
- Realizar auditorías mensuales para evaluar la eficacia del sistema de presentación de informes, luego monitorear y resolver los problemas reportados.

Anexo 5- formulario



1. Nombre completo *

Escriba su respuesta

2. Cargo *

Escriba su respuesta

3. Correo electronico *

Escriba su respuesta

4. De 0 a 10, donde 0 es la calificación más baja y 10 la calificación más alta, por favor responda las siguientes preguntas:

5. ¿Qué tan útil considera que es el marco presentado para su empresa? *

0	1	2	3	4	5	6	7	8	9	10

6. ¿Qué tan bien se abordaron sus inquietudes o preguntas durante la presentación? *

0	1	2	3	4	5	6	7	8	9	10

7. ¿Qué tan probable es que usted considere aplicar las recomendaciones del marco presentado? *

0	1	2	3	4	5	6	7	8	9	10

8. ¿Hubo algún tema que le gustaría que se hubiera tratado con más profundidad? *

Escriba su respuesta

9. ¿Hubo algún aspecto de la presentación que no le gustara o que considere mejorable? *

Escriba su respuesta

Agregar nueva pregunta

Anexo 6


¿RECIBISTE MAIL DE READ ASSITANT?
Read Assistant<executiveassistant@e.read.ai>
Para: Scarlett Omana
Vie 20/09/2
Parte del contenido de este mensaje fue bloqueado porq
seguros.
Remitente de confianza
Mostrar contenido
Haz caso omiso
Si accediste a ver el informe y creaste una cuenta. Sigue estos pasos a continuación:
La reunión se centró en la introducción de una dinámica propuesta por Carlos Ivan Maldonado Avelino, denominada "Estás en Mute". La actividad consistió en que un participante debía adivinar una frase con el micrófono apagado, mientras los demás intentaban descifrarla. La dinámica se llevó a cabo con entusiasmo y contribuyó... ver más
Acceder a este informe de la reunión
Se requiere la creación de una cuenta
Resumen
Capítulos & Temas