**Brief para Evaluación de la Campaña de Concientización en CIberseguridad**

Los siguientes son ejemplos de alternativas de evaluación de la campaña de concientización realizada. La empresa debe analizar las alternativas y seleccionar la que más se ajuste a su cultura.

Primero, clarificar los objetivos, medios utilizados y esperables de la campaña, para establecer indicadores de medición.

**Objetivos de la Campaña**

|  |
| --- |
| * x * x * x |

**¿A quienes fue dirigida la campaña?**

|  |
| --- |
| * x * x * x |

**¿Qué debiese conocer/hacer finalmente el Usuario?**

|  |
| --- |
| * x * x * x |

**Canales o medios de Distribución Utilizados**

|  |
| --- |
| * x * x * x |

**Planilla de Plan de Acción**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Iniciativa | Descripción | Audiencia | Fechas | Comentarios |
|  |  |  |  |  |
|  |  |  |  |  |

**Mecanismos alternativos de Evaluación de la Campaña**

**Definición de KPIs (Indicadores Clave de Desempeño)**

|  |
| --- |
| *La definición de KPIs permitirá evaluar no sólo el conocimiento adquirido, sino también el cambio de comportamiento y la implementación de buenas prácticas.*  ***Nivel de Conocimiento Pre y Post Campaña:***  ***Definición:****Medida del aumento en el conocimiento sobre Ciberseguridad.*  ***Objetivo SMART:****Aumentar el conocimiento (comportamiento) general en un XX% al comparar los resultados de encuestas antes y después de la campaña.*  *En Anexo, podrás encontrar sugerencias para más KPIs.* |

**Crear Instrumentos de Recolección de Datos**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Encuestas y Cuestionarios:****Crear encuestas para medir la satisfacción del cliente, la efectividad de la comunicación interna, etc. (Ejemplo propuesto)*   1. ***Antes del inicio de la campaña:*** *¿Cuán familiarizado estás con conceptos básicos de ciberseguridad como amenaza, vulnerabilidad y riesgo?*    * 1. *Nada familiarizado*      2. *Algo familiarizado*      3. *Muy familiarizado* 2. ***Después de la campaña:*** *¿Cuál es tu nivel de confianza conceptos básicos de ciberseguridad, luego de la campaña?*    * 1. *Bajo*      2. *Moderado*      3. *Alto* 3. ***Conocimientos específicos:*** *¿Entiendes cómo funcionan los conceptos vistos (cambiar a los tópicos que vimos) y su importancia en la protección de la información y redes?*    * 1. *No comprendo*      2. *Comprendo un poco*      3. *Comprendo completamente* 4. ***Cambio de comportamiento:*** *¿Con qué frecuencia revisas las configuraciones de privacidad de tus dispositivos ahora en comparación con antes de la campaña?*    * 1. *Menos frecuencia*      2. *La misma frecuencia*      3. *Más frecuencia*   *Medición de la encuesta (ejemplo): asocia un puntaje a las respuestas a); b) y c).*   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | *a) 0 pto.* | *b) 50 ptos.* | *c) 100 ptos.* | *Total de ptos.* | | *1* |  | *X* |  | *50* | | *2* |  |  | *x* | *100* | | *3* |  |  | *x* | *100* | | *4* |  | *X* |  | *50* | | ***Total*** | | | | ***300*** |   *Puntaje máximo: 400: excelente nivel de satisfacción y comprensión de la Ciberseguridad.*  *Puntaje entre 300 y 350: buen nivel de satisfacción y comprensión de la Ciberseguridad.*  *Puntaje entre 200 y 250: aceptable nivel de satisfacción y comprensión de la Ciberseguridad, se requiere refuerzo*  *Puntaje entre 50 y 150: bajo nivel de satisfacción y comprensión de la Ciberseguridad, se requiere replantear la estrategia de comunicación.*  *Puntaje mínimo: 0 nulo nivel de satisfacción y comprensión de la Ciberseguridad*  En Anexo, podrás encontrar una propuesta de encuesta, de qué tan buena fue la campaña.  ***Entrevistas y Grupos Focales:****Realizar entrevistas con partes interesadas clave para obtener información cualitativa.*  ***Formato para Entrevistas Individuales***  ***1. Introducción***   * *Presentación del entrevistador.* * *Explicación del propósito de la entrevista.* * *Aseguramiento de confidencialidad y consentimiento para registrar la conversación.*   ***2. Preguntas de Apertura***   * *¿Cómo describirías tu nivel de conocimiento sobre ciberseguridad antes de la campaña?* * *¿Qué esperabas aprender de esta campaña?*   ***3. Preguntas Centrales***   * *¿Qué aspectos de la campaña consideras más útiles? ¿Por qué?* * *¿Hubo algún tema que te pareció confuso o difícil de entender?* * *¿Cambiaste alguna práctica habitual en línea como resultado de la campaña? Si es así, ¿cuál?*   ***4. Preguntas de Cierre***   * *¿Tienes algún consejo o sugerencia para mejorar futuras campañas de sensibilización en ciberseguridad?* * *¿Te gustaría agregar algo más que no hayamos discutido?*   ***5. Conclusión***   * *Agradecer al participante por su tiempo y aportes.* * *Reafirmar la confidencialidad de sus respuestas.*   ***Formato para Grupos Focales***  ***1. Introducción***   * *Presentación del moderador.* * *Explicación del objetivo del grupo focal y las reglas básicas (ej., respeto, confidencialidad).* * *Solicitar consentimiento para grabar la sesión.*   ***2. Icebreaker***   * *Pregunta de apertura para romper el hielo: "Comparta una experiencia personal relacionada con ciberseguridad que considere importante."*   ***3. Temas de Discusión***   * ***Percepción general:****¿Cuál fue tu percepción general de la campaña de ciberseguridad?* * ***Contenido Relevante:****¿Qué temas encontraron más relevantes o impactantes?* * ***Aplicabilidad:****¿Cómo planean aplicar lo que aprendieron en su rutina diaria o laboral?* * ***Desafíos y Barreras:****¿Cuáles fueron las principales barreras para entender o implementar alguna de las prácticas sugeridas?* * ***Uso de Recursos:****¿Qué opinan de los materiales educativos proporcionados?*   ***4. Reflexión***   * *Pregunta para reflexionar: "¿Cuál es la principal lección que te llevas de esta experiencia y por qué?"*   ***5. Comentarios Finales***   * *Solicitar cualquier comentario adicional que los participantes deseen compartir.*   ***6. Conclusión***   * *Agradecer a todos los participantes por su tiempo y contribuciones.* * *Informar sobre los próximos pasos y cómo se utilizarán sus ideas para mejorar la campaña.*   *En Anexo, podrás encontrar una propuesta de encuesta, de satisfacción de la campaña.* |

**Definir Métodos de Análisis**

|  |
| --- |
| ***ANÁLISIS CUANTITATIVO***  *Utilizar análisis estadístico para interpretar datos numéricos y KPIs.*   * + 1. ***Contexto:*** *Has implementado una campaña de sensibilización en ciberseguridad en tu empresa y has recogido datos antes y después de la campaña mediante encuestas que miden el conocimiento sobre prácticas de ciberseguridad.*     2. ***Objetivo del Análisis:*** *Cuantificar la mejora en el conocimiento de los empleados sobre ciberseguridad después de la campaña.*     3. ***Datos Recogidos:*** * *Encuesta de conocimiento previa a la campaña.* * *Encuesta de conocimiento posterior a la campaña.*   + 1. ***Variables de Interés:***   + *Puntuación de conocimiento: puntaje total obtenido por cada empleado en las encuestas pre y post campaña.*   ***Pasos para el Análisis Cuantitativo (ejemplo):***   * + - 1. ***Recopilación de Datos:*** * ***Pre-campaña:****Se encuesta a 100 empleados, obteniendo una puntuación promedio de 60 sobre 100.* * ***Post-campaña:****Se encuesta a los mismos 100 empleados, obteniendo una puntuación promedio de 80 sobre 100.*   + - 1. ***Análisis Estadístico:*** * ***Cambio Promedio:****Calcular el cambio promedio en las puntuaciones de conocimiento. Cambio Promedio = Puntuación Promedio Post-campaña - Puntuación Promedio Pre-campaña= 80 - 60 = 20 puntos de mejora promedio.*   + - 1. ***Prueba de Significancia:*** * *Realizar una prueba T para muestras relacionadas (pareadas) para determinar si el cambio en el conocimiento es estadísticamente significativo.*   + ***Hipótesis Nula (H0):****No hay diferencia en el conocimiento antes y después de la campaña.*   + ***Hipótesis Alternativa (H1):****Hay una mejora significativa en el conocimiento después de la campaña.*   + *Si el valor p es menor que el nivel de significancia (por ejemplo, 0.05), rechazas H0 y concluyes que la campaña ha tenido un impacto significativo.*     - 1. ***Visualización:*** * *Crear gráficos de barras o histogramas que muestren la distribución de las puntuaciones pre y post campaña para visualizar el cambio.*   + - 1. ***Interpretación de Resultados:*** * *Si el análisis estadístico muestra significancia, puedes afirmar que la campaña mejoró significativamente el conocimiento de ciberseguridad entre los empleados.*   + - 1. ***Informe Final:*** * *Documentar los métodos, resultados y conclusiones en un informe fácil de entender para presentar a los interesados.*   ***ANÁLISIS CUALITATIVO***  *Analizar los comentarios obtenidos de entrevistas y encuestas abiertas para identificar tendencias y percepciones.*   * + 1. ***Contexto:*** *Has realizado entrevistas y encuestas abiertas con empleados al finalizar una campaña de sensibilización en ciberseguridad. Las respuestas obtenidas incluyen opiniones y experiencias personales con relación a la campaña.*     2. ***Objetivo del Análisis:*** *Identificar temas y tendencias comunes en las percepciones de los empleados sobre la campaña de ciberseguridad.*   ***Pasos para el Análisis Cualitativo:***   1. ***Recolección de Comentarios:*** *Reúne todos los comentarios obtenidos de entrevistas y preguntas abiertas en encuestas.* 2. ***Lectura Inicial:*** *Lee todos los comentarios detenidamente para obtener una comprensión general del contenido.* 3. ***Codificación:***  * *Identifica y subraya palabras o frases clave en los comentarios.* * *Asigna códigos o etiquetas a estos fragmentos textuales. Por ejemplo:*   + - *"Confusión sobre uso de herramientas": falta de claridad*     - *"Satisfacción con ejemplos prácticos": utilidad práctica*     - *"Interés en más formación sobre phishing": necesidad de más formación*  1. ***Identificación de Temas:*** *Agrupa los códigos en temas o categorías más amplias. Por ejemplo:*    * *Claridad y comprensión*    * *Aplicabilidad práctica*    * *Áreas de mejora sugeridas* 2. ***Análisis de Tendencias:*** *Examina la frecuencia y contexto de los temas identificados. Busca patrones o percepciones recurrentes entre los participantes.* 3. ***Ejemplo de Resultados:***    * + ***Claridad y Comprensión:*** *Hallazgo: Algunos empleados encontraron confusas ciertas partes del contenido, especialmente en el uso de herramientas de cifrado.*      + ***Aplicabilidad Práctica:*** *Hallazgo: La mayoría de los participantes valoró positivamente los ejemplos prácticos proporcionados, considerándolos útiles para su rutina diaria.*      + ***Áreas de Mejora:*** *Hallazgo: Muchos expresaron interés en recibir más formación específica sobre reconocimiento y prevención de ataques de phishing.* 4. ***Informe de Resultados:***    * *Resume los temas y subtemas principales identificados.*    * *Ofrece recomendaciones basadas en el análisis, como mejorar la claridad de las presentaciones o ampliar la capacitación sobre phishing.* 5. ***Validación:***    * *Revisión del análisis con colegas o participantes para asegurar que las interpretaciones sean precisas y reflejen correctamente las percepciones de los empleados.* |

**Implementación de las Herramientas**

|  |
| --- |
| ***Software de Gestión de Datos:****Implementar soluciones como hojas de cálculo avanzadas o softwares estadísticos (SPSS (Statistical Package for the Social Sciences), R, SAS (Statistical Analysis System), Stata, MATLAB, Python (con bibliotecas como Pandas, NumPy, SciPy, y Matplotlib), Minitab) para almacenar y analizar datos.*  ***Plataformas de Encuestas en Línea:****Utilizar herramientas como Google Forms, SurveyMonkey, etc., para distribuir encuestas y recolectar respuestas.* |

**Validación de Mecanismo de Evaluación**

|  |
| --- |
| ***Revisión por Pares:****Hacer que colegas revisen el mecanismo de evaluación para verificar su validez y exhaustividad.*  ***Pasos para la Revisión por Pares:***   1. ***Selección del Equipo de Revisión:***    * *Identifica un grupo de 3-5 colegas con experiencia en ciberseguridad, análisis de datos y diseño de evaluaciones.*    * *Si es posible, incluye a personas no involucradas en el desarrollo inicial del mecanismo para proporcionar una perspectiva fresca.* 2. ***Distribución de Materiales:***    * *Proporciona al equipo de revisión toda la documentación relevante, incluyendo:*      + *Los KPIs establecidos para la campaña.*      + *Las herramientas y métodos de recolección de datos.*      + *Los enfoques de análisis que se emplearán.*      + *Resultados preliminares, si están disponibles.* 3. ***Sesión de Revisión (en reunión o por escrito):***    * *Pide a los revisores que examinen cada parte del mecanismo de evaluación y proporcionen comentarios sobre los siguientes puntos:*      + ***Claridad y Precisión:****¿Son claros los objetivos de la evaluación y están correctamente alineados con los KPIs?*      + ***Cobertura:****¿Cubre el mecanismo de evaluación todos los aspectos clave de la campaña?*      + ***Validez:****¿Los métodos de recolección y análisis de datos proporcionarán resultados válidos y fiables?*      + ***Sugerencias de Mejora:****¿Hay áreas donde se podría mejorar o afinar la evaluación?* 4. ***Recopilación de Comentarios:***    * *Colecciona los comentarios escritos o discute las opiniones recogidas durante una sesión de revisión.* 5. ***Incorporación de Comentarios:***    * *Evalúa las sugerencias y comentarios de tus colegas.*    * *Implementa los cambios y mejoras sugeridos que sean viables y relevantes.* 6. ***Informe de Resultados de Revisión:***    * *Documenta el proceso de revisión, listando las mejoras realizadas y las razones de cualquier comentario que no se implementó.* 7. ***Feedforward:***    * *Realiza una última revisión con el equipo original para confirmar que las mejoras integradas son satisfactorias y completas.* |

**ANEXOS**

|  |
| --- |
| ***En este apartado, podrás encontrar sugerencias para completar las herramientas de evaluación***  ***Para completar KPIs, te sugerimos lo siguiente:***  ***Participación en Talleres y Seminarios:***  ***Definición:****Porcentaje de empleados que asisten a eventos de capacitación en ciberseguridad.*  ***Objetivo SMART:****Lograr que al menos el 85% de los empleados asistan a un evento de capacitación dentro del periodo de la campaña.*  ***Tasa de Corrección de Vulnerabilidades Reportadas:***  ***Definición:****Porcentaje de vulnerabilidades corregidas tras ser reportadas durante simulaciones de pentesting (test de penetración está diseñado para determinar el alcance de los fallos de seguridad de un sistema.)*  ***Objetivo SMART:****Corregir el 100% de vulnerabilidades críticas identificadas dentro de los 15 días posteriores al reporte.*  ***Reducción de Incidentes de Phishing:***  ***Definición:****Disminución del número de incidentes exitosos de phishing reportados.*  ***Objetivo SMART:****Reducir los incidentes de phishing exitosos en un 50% durante el trimestre siguiente a la campaña.*  ***Evaluaciones de Resiliencia y Seguridad (ISO/IEC 27001):***  ***Definición:****Resultados de auditorías internas respecto al cumplimiento de la norma ISO/IEC 27001.*  ***Objetivo SMART:****Aumentar el cumplimiento de los controles ISO en un 20% en un año.*  ***Índice de Reportes de Seguridad Activos:***  ***Definición:****Aumento en el número de reportes de incidentes de seguridad, mostrando sensibilización y proactividad.*  ***Objetivo SMART:****Incrementar los reportes en un 70%, indicando mayor conciencia y participación del personal.*  ***Mejora en las Prácticas de Gestión de Identidades y Accesos (IAM - Identity and Access Management):***  ***Definición:****Evaluación de la implementación efectiva de políticas IAM.*  ***Objetivo SMART:****Alcanzar un cumplimiento del 95% en las auditorías de IAM dentro de seis meses.*  ***Intervenciones Preventivas del SOC (Security Operations Center -*** *Es una función en la gestión de ciberseguridad que está dedicada a monitorear, detectar y responder a incidentes de seguridad en una organización.):*  ***Definición:****Número de amenazas detectadas y neutralizadas por el SOC antes de convertirse en incidentes.*  ***Objetivo SMART:****Aumentar las intervenciones preventivas en un 40% dentro del primer año de implementación de mejoras.*  ***Mejora en la Configuración de Firewalls y Cifrado:***  ***Definición:****Evaluación de la efectividad en la implementación de firewalls y cifrado de datos.*  ***Objetivo SMART:****Auditar mensualmente y mantener un 98% de cumplimiento en configuraciones efectivas.*  ***Eficiencia de la Respuesta ante Incidentes:***  ***Definición:****Tiempo promedio de respuesta y resolución de incidentes de seguridad.*  ***Objetivo SMART:****Reducir el tiempo de respuesta a menos de 10 minutos en seis meses.*  ***Si necesitas completar la encuesta de satisfacción aquí te dejamos una sugerencia de satisfacción de la campaña.***  ***Encuesta de Satisfacción con la Campaña:***   * + 1. ***Calidad de la información proporcionada:*** *¿Cómo calificarías la claridad y utilidad de la información proporcionada durante la campaña?*     2. *Pobre*     3. *Adecuada*     4. *Buena*     5. *Excelente*  1. ***Relevancia de los temas abordados:*** *¿Consideras que los temas tratados (como phishing, malware, cifrado, etc.) fueron relevantes y útiles para tu trabajo diario?*    * 1. *Nada relevante*      2. *Poco relevante*      3. *Moderadamente relevante*      4. *Muy relevante* 2. ***Opinión sobre las actividades de capacitación:*** *¿Qué tan efectivas fueron las actividades prácticas (talleres, simulaciones, etc.) en ayudarte a comprender los conceptos de seguridad?*    * 1. *Nada efectivas*      2. *Poco efectivas*      3. *Efectivas*      4. *Muy efectivas* 3. ***Satisfacción general:*** *En general, ¿qué tan satisfecho estás con la campaña de sensibilización?*    * 1. *Muy insatisfecho*      2. *Insatisfecho*      3. *Neutral*      4. *Satisfecho*      5. *Muy satisfecho* 4. ***Comentarios adicionales:*** *¿Tienes alguna sugerencia para mejorar futuras campañas de ciberseguridad?*   *[Campo de texto libre]*  ***Para complementar Listas de Verificación (Checklists), te sugerimos considerar lo siguiente:***   * + - 1. ***Material Educativo y Recursos*** * *Crear documentos de referencia sobre conceptos básicos (amenazas, vulnerabilidades, etc.)* * *Preparar guías y consejos prácticos sobre:*   + *Uso adecuado de contraseñas.*   + *Técnicas para reconocer correos electrónicos de phishing.*   + *Uso de firewalls y herramientas de cifrado.* * *Distribuir material educativo a todos los participantes.*   + 1. ***Ejecución de la Campaña*** * *Realizar sesiones de entrenamiento obligatorias para todos los empleados.* * *Implementar simulaciones de ataque (ej., phishing) para evaluar la preparación.* * *Configurar y utilizar un canal de comunicación para dudas y consultas de los participantes.*   + 1. ***Evaluación y Medición*** * *Distribuir encuestas de pre-campaña para evaluar el conocimiento inicial.* * *Realizar evaluaciones al final de cada módulo o sesión.* * *Aplicar encuestas de post-campaña para medir el conocimiento adquirido y la satisfacción.*   + 1. ***Seguimiento y Mejora Continua*** * *Analizar los resultados de las encuestas y simulaciones para identificar áreas de mejora.* * *Generar un informe final detallado con los hallazgos y recomendaciones.* * *Planificar sesiones de refuerzo regular para mantener el conocimiento actualizado.*  1. ***Cumplimiento y Reporte***  * *Verificar que todos los participantes han completado las actividades asignadas.* * *Documentar cualquier incidente detectado durante la campaña.* * *Ajustar las políticas y procedimientos en base a los hallazgos de la campaña.*   ***A continuación, te sugerimos que generes un calendario de cómo recolectarás los datos de la campaña, aquí te entregamos el siguiente ejemplo:***  ***Recolectar Datos:****Seguir un calendario de recolección de datos para asegurar consistencia y cobertura completa.*  ***Fase 1: Antes del Lanzamiento de la Campaña***   * ***Semana 1 y 2:***   + *Realizar una encuesta de conocimiento inicial a todos los empleados (pre-test).*   + *Recolectar datos demográficos básicos para segmentar los resultados.*   ***Fase 2: Durante la Implementación de la Campaña***   * ***Semana 3:***   + *Realizar un taller sobre amenazas y vulnerabilidades.*   + *Distribuir una breve encuesta de reacción inmediata al final del taller para evaluar la comprensión y satisfacción.* * ***Semana 4:***   + *Simulación de ataque de phishing.*   + *Registrar la tasa de respuesta incorrecta (empleados que hicieron clic en el enlace falso).* * ***Semana 5:***   + *Sesión de capacitación sobre ingeniería social y técnicas de phishing.*   + *Recolectar comentarios cualitativos a través de grupos focales.*   ***Fase 3: Inmediatamente Después de la Campaña***   * ***Semana 6:***   + *Administrar el post-test de conocimiento general para comparar con la encuesta inicial.*   + *Introducir encuestas de satisfacción para evaluar el impacto percibido de la campaña.*   ***Fase 4: Seguimiento Post-Campaña***   * ***Mes 3 Post-Campaña:***   + *Recolección de datos de incidentes de ciberseguridad reportados tras la campaña.*   + *Evaluar cambios en la frecuencia de incidentes y respuestas proactivas de los empleados.* * ***Mes 6 Post-Campaña:***   + *Realizar una evaluación adicional del conocimiento para medir la retención a largo plazo.*   + *Preparar un informe comparativo de las métricas de seguridad antes, durante y después de la campaña.*   ***Una vez realizada la campaña, has recopilado datos, que requieren ser analizados, a continuación, te entregamos algunos pasos de ejemplo, que te ayudarán en el análisis***  ***Datos Recolectados:***   * *Pre-test y post-test de conocimiento.* * *Datos sobre incidentes de phishing antes y después de la campaña.* * *Resultados de encuestas de satisfacción tras la campaña.*   ***Pasos para Analizar los Datos:***   1. ***Evaluación del Conocimiento Incrementado:***    * *Calcular el aumento porcentual en las puntuaciones de conocimiento desde el pre-test al post-test.*      + *Dato Pre-test promedio: 60/100*      + *Dato Post-test promedio: 80/100*      + *Incremento de conocimiento: ((80-60)/60) \* 100 = 33.3%*    * *Comparación con KPI: El aumento del 33.3% supera el objetivo de 25%, indicando un logro significativo en esta área.* 2. ***Reducción de Incidentes de Phishing Exitoso:***    * *Comparar el número de incidentes reportados antes y después de la campaña.*      + *Antes de la campaña: 40 incidentes exitosos por mes.*      + *Después de la campaña: 18 incidentes exitosos por mes.*      + *Reducción porcentual: ((40-18)/40) \* 100 = 55%*    * *Comparación con KPI: La reducción del 55% excede la meta del 50%, mostrando un impacto positivo.* 3. ***Satisfacción de los Participantes:***    * + *Analizar las respuestas a la encuesta de satisfacción: El 92% de los encuestados expresó estar satisfecho o muy satisfecho con la campaña.*    * *Comparación con KPI: Con un 92%, el KPI del 90% de satisfacción ha sido cumplido exitosamente.* 4. ***Informe de Resultados:***    * *Documentar cada análisis y resultado en un informe que incluya comparaciones visuales (gráficos de barras, líneas de tiempo).*    * *Incluir cualquier comentario adicional obtenido de análisis cualitativos para complementar los hallazgos cuantitativos.* 5. ***Conclusiones y Recomendaciones:***    * *Con base en los análisis, concluir que la campaña ha superado los objetivos establecidos.*    * *Recomendar mantener o ajustar ciertas estrategias para continuar mejorando la ciberseguridad en la organización.* |