

Whitepaper

CÓMO DESARROLLAR UNA CAPA DE SEGURIDAD ORIENTADA AL USUARIO



Índice

01	INTRODUCCIÓN	3
02	DEFINICIÓN DEL PROYECTO	4
03	PROCESOS DE HARDENING DE USUARIOS	5
	3.1. Concientización Y Entrenamiento	5
	Contenidos	5
	Forma De Presentación	6
	3.2. Evaluación	7
	Evaluación De Conocimientos	7
	Evaluación De Hábitos Y Comportamientos	7
04	EJECUCIÓN DEL PROYECTO	9
	4.1. Establecer una línea base	9
	4.2. Planificar acciones	9
	4.3. Preparar a los usuarios	10
	4.4. Ejecutar el plan	10
	4.5. Registrar acciones	10
05	MEJORA CONTINUA	11
06	OTROS BENEFICIOS	12
	6.1. Cumplimiento	12
	6.2. Privacidad	12
	6.3. Imagen del área de seguridad	13
	6.4. Mejora en la ejecución de procesos	13
07	CONCLUSIÓN	14

1. Introducción

En esta guía describiremos cómo desarrollar **una capa de seguridad de la información orientada a las personas**. Para conocer por qué querría alguien incluir a las personas en su estrategia de seguridad de la información, puede leer los siguientes artículos:

- ¿Por qué eres el único responsable de la seguridad de la información? (Y cómo dejar de serlo)
- ¿Seguimos desconfiando del usuario final o hacemos algo al respecto?
- Todos los números indican que es hora de Concientizar
- El Arte de Engañar al Usuario - Parte 5: Medidas de Protección

Para desarrollar nuestra capa de seguridad, llevaremos adelante un **proyecto de Hardening de Usuarios**. Este término tiene su origen en los procesos de Hardening que se aplican habitualmente en las organizaciones y consisten en asegurar un sistema operativo, servidor o aplicación, reduciendo sus vulnerabilidades o agujeros de seguridad. **Como los usuarios también son parte de los sistemas de información de las organizaciones y tienen sus propias vulnerabilidades** - que son explotadas a diario por los ciberdelincuentes alrededor del mundo - es necesario incluirlos también en un proceso de Hardening, el cual se definirá en detalle a lo largo de este artículo.

Los sistemas de información se conforman de información, procesos y personas que, típicamente, pero no siempre, interactúan con sistemas informáticos.

Las personas, en particular, son consideradas el eslabón más débil de la cadena de seguridad, y existen muchas maneras de explotar sus vulnerabilidades.

CISSP All-in-one 7th. Edition



2. Definición del proyecto

Antes de comenzar cualquier proyecto de Seguridad de la Información, es indispensable que contemos **con el apoyo de la alta gerencia de nuestra organización**. Contar con su apoyo significa contar con el soporte, presupuesto, tiempo y recursos necesarios para llevar adelante nuestro proyecto según el alcance y los objetivos que hayamos definido para el mismo.

Por lo tanto, lo primero que debemos hacer es definir nuestro proyecto de Hardening de Usuarios y conseguir su aprobación por parte de la alta gerencia de nuestra organización. **Es muy importante definir** claramente en este punto el **alcance del proyecto**, si incluimos a toda nuestra organización, o sólo una parte, o si vamos a abarcar también otras sucursales o territorios.

Es recomendable incluir desde el principio al área de Recursos Humanos en el proyecto de Hardening de Usuarios. Esto es así ya que estaremos trabajando directamente con las personas de nuestra organización, y los procesos de Recursos Humanos, como por ejemplo, las contrataciones, influirán directamente en los procesos de Hardening de Usuarios.



Sin el apoyo de la alta dirección, un programa de seguridad no va recibir la atención, fondos, recursos y capacidad de ejecución necesarios para ser llevado adelante"

CISSP All-in-one 7th. Edition

3. Proceso de Hardening de usuarios

Un proyecto de Hardening de Usuarios consta básicamente de dos procesos, los cuales son:

- **Concientización y Entrenamiento:** Orientado al desarrollo de hábitos y comportamientos seguros de los usuarios.
- **Evaluación:** Orientado a la medición de los hábitos y comportamientos desarrollados.

A continuación, se describe en detalle cada uno de ellos:

3.1 Concientización y entrenamiento

Este proceso será el encargado de crear los conocimientos, hábitos y comportamientos seguros de los usuarios de nuestra organización. Es importante remarcar que no estamos hablando simplemente de asimilación de conocimientos sólo desde un punto de vista académico, por ejemplo, que un usuario sencillamente sepa qué es el Phishing, sino que, ante una trampa de este tipo, se comporte de manera segura y no comprometa su información personal ni la de la organización.

Contenidos

Los contenidos son una pieza clave dentro del proceso de Concientización y Entrenamiento. Cuando hablamos de contenidos nos referimos al material que se presentará a los usuarios para concientizarlos y entrenarlos.

Contenido principal

Es el material que se utiliza para brindar las principales capacitaciones a los usuarios. Suele cubrir en forma detallada uno o más tópicos.

Este material debe resultar atractivo para los usuarios, ya que estamos presentando contenido que muy probablemente no es de su interés. Idealmente, no debería presentar conceptos directos ni imponer directivas. En cambio, se debería ubicar a los usuarios en diversos escenarios cotidianos de su día a día, dentro de los cuales puedan sentirse identificados, y mostrar cuál es la conducta segura en cada uno de ellos. Lo más recomendable para lograr un cambio de comportamiento es entregar valor a través del refuerzo positivo y consejos, y hablar de cómo lo aprendido impacta en la vida personal de cada usuario, utilizando un lenguaje cercano a éste.

✓ **Contenido de refuerzo**

Es aquel que sirve para reforzar el contenido principal. Las personas no tienen una memoria perfecta, y menos aún son propensas a recordar algo que no es de su total interés. No podemos explicar un día a un usuario cómo comportarse frente a una URL acortada y esperar que lo recuerde dentro de dos meses por ejemplo. Incluso, ya el día siguiente habrá olvidado un porcentaje amplio de la información que le dimos.

Por eso es importante reforzar el contenido previamente enseñado a los usuarios. Las acciones de refuerzo no deben intentar abarcar el 100% del contenido principal, sino recordar periódicamente pequeños extractos para mantenerlos alertas y mejorar la asimilación del contenido.

Forma de presentación

Además de disponer de los contenidos, debemos tener en cuenta la manera en que los presentaremos a nuestros usuarios.

✓ **Contenido principal**

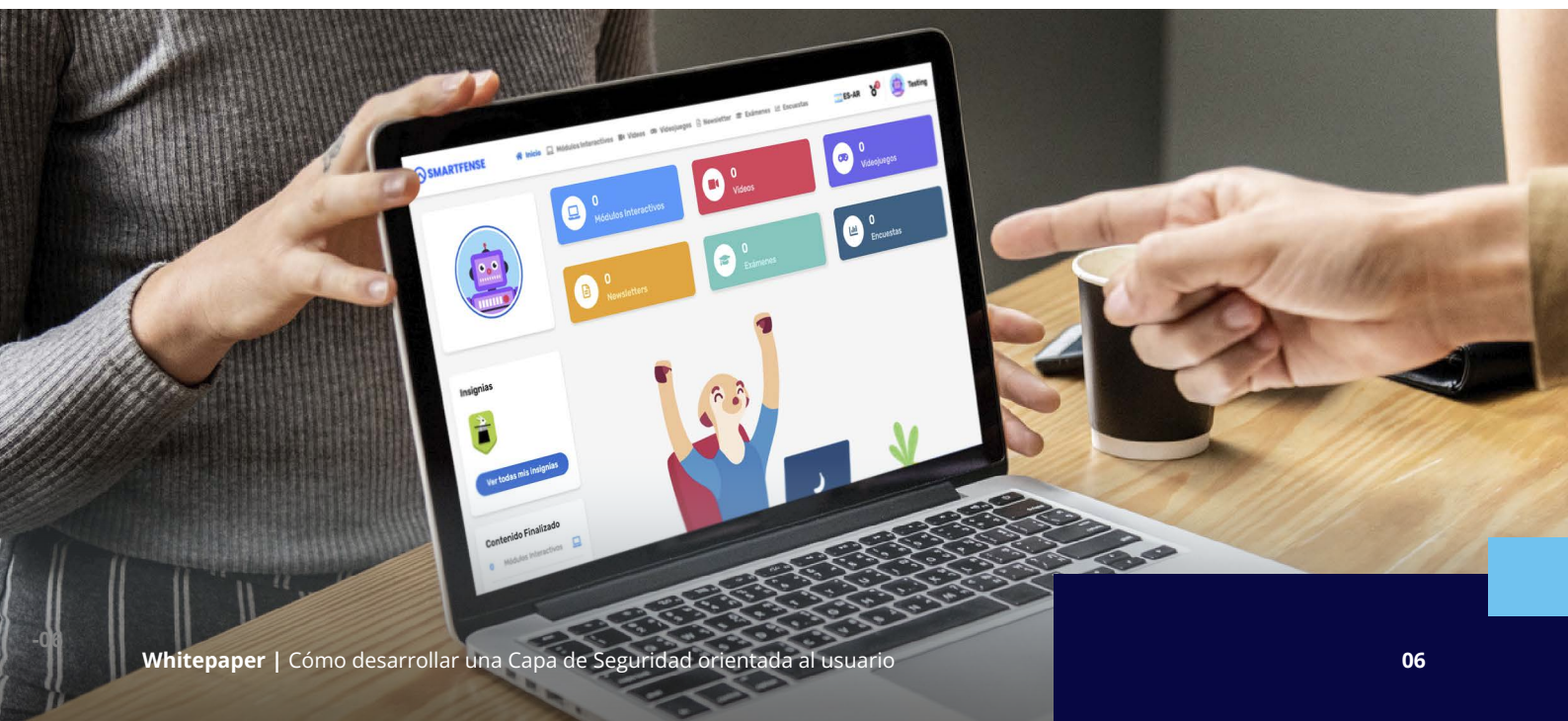
La manera ideal de presentar el contenido principal es, como ya se mencionó, de una forma que sea atractiva para los usuarios. Principalmente, podrá realizarse mediante:

- Capacitaciones presenciales
- Capacitaciones a través de recursos tecnológicos

En ambos casos, lo más importante es que el usuario tenga un grado alto de interacción y se vea motivado a completar el entrenamiento.

✓ **Contenido de refuerzo**

Algunas formas de presentar el contenido de refuerzo son:



- Newsletters
- Posters
- Fondos de pantalla
- Protectores de pantalla
- Videos resumen
- Infografías
- Folletos o Volantes
- Calendarios
- Artículos
- Regalos
- Comics

3.2. Evaluación

La medición es una parte indispensable de un proyecto ya que nos permite determinar el grado de **efectividad** que tienen nuestras acciones para el cumplimiento de nuestros objetivos.

Para el caso que nos confiere, dicha medición será realizada dentro del proceso de evaluación. Específicamente, este proceso nos servirá para mensurar los conocimientos, hábitos y comportamientos de nuestros usuarios antes de, y durante, la Concientización y Entrenamiento.

Evaluación de conocimientos

La evaluación de conocimientos es la forma más tradicional de medición en un proceso de Concientización y Entrenamiento.

Básicamente, lo que se **determinará es el grado de asimilación de conocimientos y conceptos de Seguridad de la Información**. Para lograrlo, se suele hacer uso de exámenes, en cualquiera de sus formas, siendo algunas de ellas:

- Cuestionarios
- Múltiple Opción
- Verdadero o Falso
- Completar crucigramas

Evaluación de hábitos y comportamientos

Para evaluar los hábitos y comportamientos de nuestros usuarios, debemos ir un paso más allá y **utilizar técnicas de medición más modernas** que las mencionadas en el punto anterior.



Información Recomendada:

- > ¡Los usuarios no tienen sentido común!
- > El cambio de comportamiento y una (de muchas) técnica para lograrlo.
- > Ludificación: una herramienta ideal para complementar tu proceso de concientización en seguridad.
- > Aprendizaje basado en juegos: Cómo lograr un entrenamiento más divertido y eficaz para tus usuarios finales.

✓ Simulaciones

Las simulaciones nos permiten **realizar un enfoque de evaluación muy particular**. En lugar de preguntar a un usuario si conoce los peligros de un enlace acortado recibido por email, lo que haremos será enviarle un email con un enlace acortado para ver cómo se comporta frente al mismo.

Esta técnica por lo tanto consiste en poner a los usuarios en una situación de riesgo controlada, y evaluar cuál es su comportamiento frente a la misma.

Podemos realizar simulaciones de todo tipo, como por ejemplo envío de correos de suplantación de identidad con archivos adjuntos peligrosos, correos de suplantación de identidad con enlaces peligrosos, dejar memorias USB “perdidas” con archivos peligrosos, etc.

Cada simulación nos permitirá medir diferentes comportamientos de nuestros usuarios, y sus resultados nos permitirán determinar si nuestras acciones de Concientización y Entrenamiento están siendo efectivas y van por buen camino, qué usuarios o áreas de nuestra organización son las más riesgosas, qué tópicos debemos reforzar, etc.

Además, podremos contar con las métricas necesarias para poder realizar reportes objetivos a la alta gerencia, justificar nuestra inversión en Hardening de Usuarios, ayudar al cumplimiento de normativas, entre otras cosas.

✓ Correlación de estadísticas

Otro método, un tanto más indirecto, para evaluar hábitos y comportamientos, es buscar la correlación de éstos con estadísticas de la organización en cuanto a otras capas de seguridad, como ser por ejemplo:

- Estadísticas de incidentes
- Estadísticas de programas antivirus
- Estadísticas de programas DLP
- Estadísticas de navegación

Por ejemplo, si la tasa de detecciones de nuestro programa antivirus comienza a disminuir al iniciar un proceso de Concientización y Entrenamiento, podemos concluir que los hábitos de nuestros usuarios se están tornando más seguros.



Información Recomendada:

- Retorno de inversión en capacitación y concientización de Seguridad de la Información.
- ¿Cuánto duran las campañas de Phishing?



4. Ejecución del proyecto

Hasta aquí hemos remarcado la necesidad de obtener la aprobación de la alta gerencia antes de embarcarnos en nuestro proyecto de Hardening de Usuarios, y hemos descrito sus procesos y componentes.

A continuación, veremos una metodología que nos permitirá reunir todos los elementos vistos y llevar adelante el proyecto:

4.1. Establecer una línea base

En materia de Seguridad de la Información es muy probable que los usuarios de nuestra organización posean conocimientos, hábitos y comportamientos muy dispares. Es por eso que es recomendable medir todos estos factores como primer paso del proyecto de Hardening de Usuarios para así establecer una línea base que represente el estado actual de nuestros usuarios.

Para establecer esta línea base, pueden utilizarse las recomendaciones que se detallan en la sección 3.2.

4.2. Planificar acciones

A partir de la línea base identificada en el punto anterior, estaremos en condiciones de planificar las acciones tanto de Concientización y Entrenamiento como de Evaluación a seguir para pasar del estado actual al estado deseado según los objetivos de nuestro proyecto.

Debemos tener en cuenta que **el material de concientización debería ser repartido a lo largo de un período extenso**, siendo planificado idealmente de manera anual. De esta forma, cada entrega ocuparía sólo una pequeña parte del tiempo del usuario, y éste no vería al proceso como un obstáculo, de modo que podría realizar en tiempo y forma sus obligaciones diarias. Además, se lograría una mejor atención y predisposición frente a los contenidos.

4.3. Preparar a los usuarios

Dependiendo de la cultura de cada organización, **habrá una mayor o menor resistencia a la hora de comenzar con el proyecto de Hardening de Usuarios**. En base a esto, puede ser necesario realizar una preparación de los usuarios previa al inicio de nuestros procesos.

Dicha preparación, implica explicar a los usuarios por qué serán incluidos en este nuevo proyecto, cuáles son los objetivos del mismo, qué herramientas van a utilizarse, cómo se utilizan dichas herramientas, y cualquier detalle que sea necesario para que enfrenten esta nueva actividad con la menor dificultad y resistencia posible.

4.4. Ejecutar el plan

Con los usuarios ya preparados, es posible comenzar a ejecutar el plan, llevando a cabo tanto las acciones de Capacitación y Entrenamiento como las Evaluaciones correspondientes.

4.5. Registrar acciones

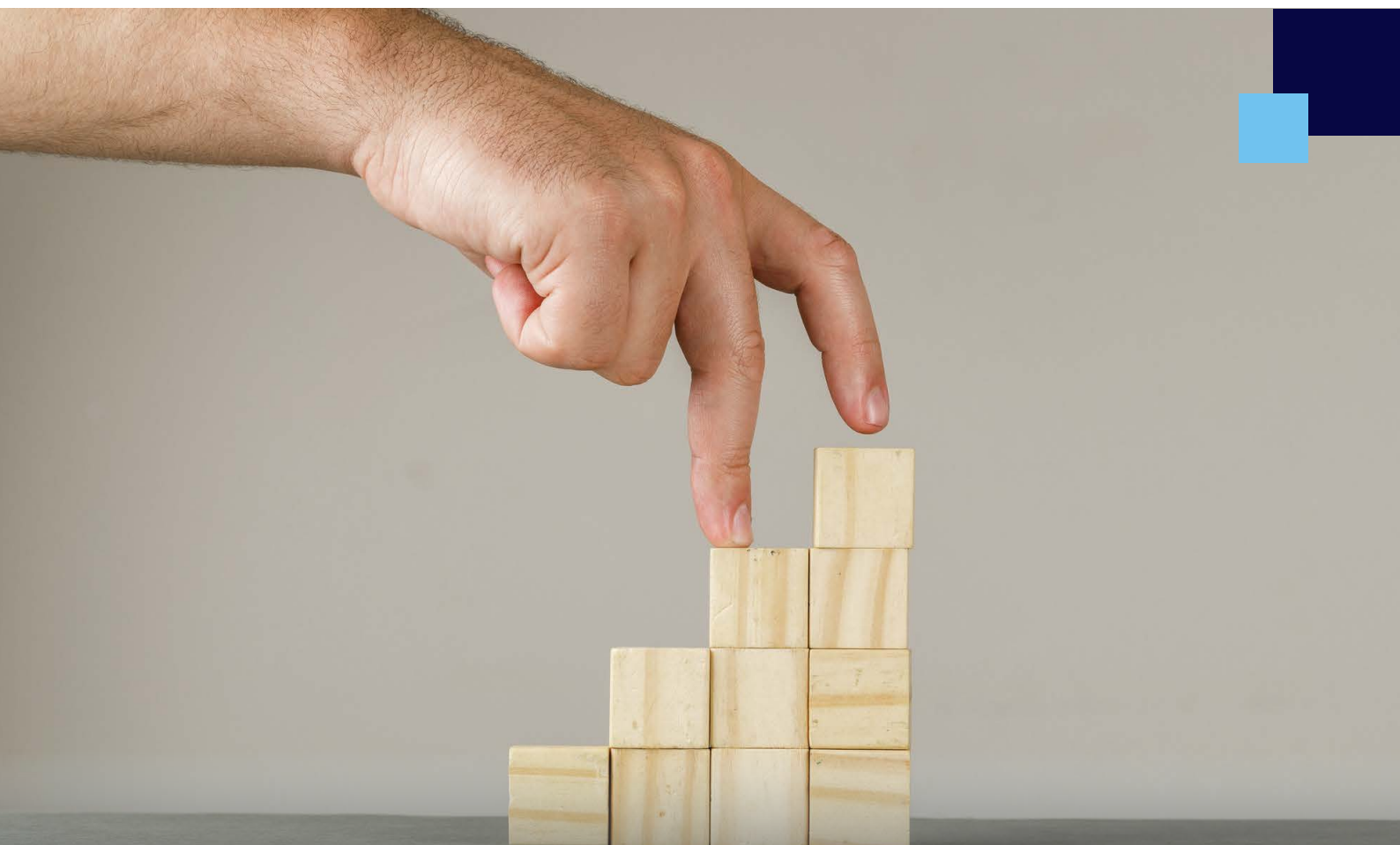
Es recomendable que **todas las acciones** que ocurran dentro de un proyecto de Hardening de Usuarios **queden registradas**. Tanto aquellas realizadas por nosotros, quienes llevamos adelante el proyecto, como las correspondientes a cada uno de los usuarios de nuestra organización. Este tipo de registros es conocido como pistas de auditoría, y su valor queda plasmado en la sección 6 de este artículo.

5. Mejora continua

La Seguridad de la Información se encuentra en constante evolución. Continuamente avanzan tanto las medidas de protección como las amenazas a la información.

Los procesos de Hardening de Usuarios deberían ser por lo tanto, procesos de mejora continua dentro de una organización. Idealmente, **el proceso de Concientización y Entrenamiento debería evolucionar y adaptarse continuamente**, tomando como entrada sus propias estadísticas, el resultado de los procesos de evaluación, y el estado del arte de la Seguridad de la Información.

La continuidad de los procesos de Hardening de Usuarios logran además mantener a todos los usuarios atentos y actualizados, y nuestra capa de seguridad orientada a las personas no se ve perjudicada por la llegada de nuevo personal a la organización, ya que también serán incluidos en el proceso.



6. Otros beneficios

Un proyecto de Hardening de Usuarios puede tener importantes beneficios extra además del desarrollo de una muy importante capa de seguridad para una organización. A continuación se mencionan algunos de ellos:

6.1. Cumplimiento

La Concientización es un requisito y un medio para el cumplimiento de diversas normativas de Seguridad de la Información, como por ejemplo:

- ISO/IEC 27001
- CobiT
- Leyes de protección de datos personales
- Estándares específicos de la industria

Para poder dar cumplimiento a dichas normas, el proceso de Concientización y Entrenamiento deberá contar con los tópicos mencionados en ellas a ser asimilados por los usuarios, pero también poseer las pistas de auditoría que permitan demostrar con registros precisos que los usuarios han sido debidamente formados y concientizados.



Información Recomendada:

- Ley de Protección de Datos Personales: Capacitación y Concientización como Requisito
- Security Awareness según la ISO/IEC 27001:2013

6.2 Privacidad

Un proceso de Concientización y Entrenamiento puede incluir la concientización de los usuarios de la organización acerca de su expectativa de privacidad. Contar con registros de auditoría que demuestren que un usuario ha sido debidamente informado respecto a su expectativa de privacidad puede marcar la diferencia dentro de un proceso legal en que la privacidad de un usuario esté en tela de juicio.

6.3. Imagen del área de seguridad

Incluir a los usuarios en la estrategia de seguridad de la organización, hará que el área sea vista con mejores ojos por parte de ellos. Esto es así ya que, en lugar de llenar a los usuarios de trabas y controles, se les está demostrando su importancia y se les está dando conocimiento útil para cuidar la información que utilizan tanto en su ámbito laboral como personal.

6.4. Mejora en la ejecución de procesos

El proceso de Concientización y Entrenamiento puede redundar en la mejora en la ejecución de otros procesos de la organización. Por ejemplo, puede concientizarse y entrenarse a los usuarios de la organización acerca del Plan de Recuperación ante Desastres de la misma. De esta manera, la organización no sólo da a conocer dicho plan ante todos sus usuarios, sino que se asegura de que, al momento de llevar dicho plan a la práctica, cada uno sepa cómo comportarse, y el plan tenga un mayor nivel de éxito.

7. Conclusión

En el presente artículo se describieron los elementos necesarios para llevar adelante un proyecto de Hardening de Usuarios. La ejecución final de dicho proyecto variará en complejidad de organización en organización, pero estos elementos deberán estar presentes para desarrollar y mantener con éxito nuestra capa de seguridad orientada a las personas.

Siempre es recomendable contar con una **herramienta** que asista en este proyecto, y que idealmente **integre los procesos de Concientización y Entrenamiento y de Evaluación**, además de incluir los contenidos apropiados para los usuarios de la organización.

Esto aliviará en gran medida al responsable de llevar adelante el proyecto debido a la automatización de tareas, la tranquilidad de contar con cobertura temática y la disponibilidad de registros confiables.



