Security Awareness Roadmap

Just like computers, people store, process, and transfer information. However, very little has been done to secure this "human" operating system, or HumanOS. As a result, people rather than technology are now the primary attack vector. Security awareness training is one of the most effective ways to address this problem. This roadmap is designed to help your organization build, maintain and measure a high-impact security awareness program that reduces risk by changing people's behavior and also meets your legal, compliance, and audit requirements. To use this roadmap, first identify the maturity level of your security awareness program and where you want to take it. Then follow the detailed steps to get there.

1 No Awareness Program

Program does not exist. Employees have no idea that they are a target, do not know or understand organizational security policies, and easily fall victim to cyber or human-based attacks.

2 Compliance Focused

Program designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad-hoc basis. Employees are unsure of organizational policies, their role in protecting their organization's information assets, and how to prevent, identify, or report a security incident.

How To Get There:

- Identify compliance or audit standards that your organization must adhere to.
- Identify security awareness requirements for those standards, which will likely require coordination with compliance or audit officer.
- Develop or purchase training to meet those requirements.
- Deploy security awareness training.
- Track who completes training, and when.

Deliverables:

- Annual training materials such as videos, newsletters and on-site presentations.
- Reports of who has and who has not completed required training.

Standards Requiring Awareness Training

- ISO/IEC 27002 §8.2.2
- PCI DSS §12.6
- SOX §404(a).(a).(1)
- GLBA §6801.(b).(1).(3)
- FISMA §3544.(b).(4).(A).(B)
- HIPAA §164.308.(a).(5).(i)
- NERC §CIP-004-3(B)(R1)
- EU Data Protection Directive

3 Promotes Awareness & Change

Program identifies the training topics that have the greatest impact in supporting the organization's mission and focuses on those key topics. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, employees, contractors and staff understand and follow organizational policies and actively recognize, prevent and report incidents.

How To Get There:

- Begin by identifying stakeholders in your organization. These are the individuals who are key to making your program a success. Once identified, build and execute a plan to gain their support. Methods to gain support include a human risk survey, awareness assessments, root cause analysis of recent incidents, industry reports or cost-benefit analysis.
- Create a baseline of your organization's security awareness level, such as with a human risk survey or phishing assessment. For additional examples refer to the Metrics section.
- Create a Project Charter that gives you authorization to begin the planning process. The Project Charter should set key expectations including identifying the project manager, cost estimates, program scope, goals, milestones, and assumptions.
- Have management review the Project Charter. Once it is approved, planning can officially begin.
- Establish a Steering Committee to assist in planning, executing, and maintaining the awareness program. Steering Committee should include 5-10 volunteer advisors from different departments or business units within your organization.
- Identify WHO you will be targeting in your program. Different roles may require different or additional training, including employees, help desk, IT staff, developers, and senior leadership.
- Identify WHAT you will communicate to the different groups targeted by your program. The goal is to create the shortest training possible that has the greatest impact. Begin with a risk analysis to identify the different human-based risks to your organization, document those risks in a matrix, and then prioritize the risks from high to low. Then select which risks you will address in your program based on priority level, time restrictions and other organizational requirements. Create a separate Learning Objectives document for each topic that identifies the different behaviors you need to change.
- Once you have determined WHO is the target of your awareness program and WHAT you will teach them, determine HOW you will communicate that content. To create an engaging program focus on how people will benefit from the training, how most of the lessons apply to their personal lives. There are two categories of training: Primary and Reinforcement. Primary training teaches new content and is usually taught annually or semi-annually and either onsite or online. Reinforcement training is employed throughout the rest of the year to reinforce key topics. Common examples of reinforcement training include newsletters, posters, podcasts, assessments and blogs. When teaching a specific topic, refer to that topic's Learning Objectives document to determine what content to communicate. This way regardless of the different ways you communicate a topic, the message will always be consistent.
- Create an execution plan in coordination with your Steering Committee. The plan should begin with WHY you are launching a security awareness program and its goals and overall scope. Then document WHO you will target in your awareness program, WHAT you will teach them and HOW. Include a timeline that identifies key milestones and the launch date of the program, critical resources involved and any other relevant information your organization may require for planning purposes.
- Have management review the plan. Once the plan is approved, you can execute your awareness program. Have the most senior stakeholder (such as your CEO) announce the program to the organization, such as by email, blog posting, or taped video.

Deliverables:

- Stakeholder matrix
- Gaining stakeholder support presentation
- Human risk survey
- Project Charter
- Steering Committee matrix
- Topics matrix
- Learning objectives document for each topic
- Execution plan

4 Long-Term Sustainment

Program has processes and resources in place for a long-term life cycle, including at a minimum an annual review and update of both training content and communication methods. As a result, the program is an established part of the organization's culture and is current and engaging.

How To Get There:

- Identify when you will review your awareness program each year.
- Identify new or changing technologies, threats, business requirements, or compliance standards that should be included in your annual update.
- Conduct an assessment of your organization's security awareness level and compare that to the baseline taken in stage 3.
- Survey staff for feedback, including what elements they liked best about the program, what needs to be changed, which topic they found most interesting, and which behaviors they changed.
- Review all the topics you are communicating and identify if new topics need to be added, and which existing topics should be removed or updated.
- Once topic changes have been identified, review and update the learning objectives for each topic.
- Review how the topics are communicated, which methods have had the greatest impact, and which need to be updated or dropped.
- Conduct an annual review and update of the budget to address changing business objectives.

Deliverables:

- Content tracking matrix used to document which topics and learning objectives were updated, by whom, and when.

5 Metrics Framework

Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. In addition, some set of metrics will be used in previous stages.

How To Get There:

- Identify key metrics that relate to business outcomes.
- Document how and when you intend to measure the metrics.
- Identify who to communicate results to, when, and how.
- Execute metrics measurement.

Deliverables:

- Metrics matrix

Examples of Metrics:

- No. of people who fall victim to monthly phishing assessments.
- No. of monthly infected systems.
- No. of monthly incidents reported.
- No. of people who completed the awareness training.
- No. of weak or shared passwords.
- Employee scores from before/after testing.
- % of users sampled with positive attitude towards information security.
- % of users sampled who believe their actions can have an impact on security.

Additional Materials:

- **NIST SP800-50**
  Building an Information Technology Security Awareness and Training Program
- **ENISA Awareness Guide (2010)**
  How to Raise Information Security Awareness
- **20 Critical Controls**
  Twenty Critical Security Controls for Effective Cyber Defense

About the Poster

This roadmap was developed as a consensus project by security professionals actively involved in security awareness programs. If you have any suggestions or would like to get involved please contact community@securingthehuman.org

Contributors Include: Randy Marchany (Virginia Tech), Cortney Stephens (Union Gas), Julie Sobel (Alliance Data), Tonia Dudley (Honeywell), John Andrew (Honeywell), Pieter Danhieux (BAE Systems Detica), Vivian Gemand (Corning), Christopher Ipsen (State of Nevada), Jenn Lesser (Facebook), Mark Merkow (PayPal), Sam Segran (Texas Tech University), Tracy Grunig (Arizona State University), Geordie Stewart (Risk Intelligence), Greg Aurigemma (Flight Safety), Janet Roberts (Progressive Insurance), Chris Sorensen (GE Capital), Mary Naphen (Lincoln Financial Group), David Vaughn (HP Enterprise Services), Tim Harwood (BP), Tanja Craig (BP), Dave Piscitello (ICANN), Eric Phifer (Seacost National Bank), Antonio Merola.

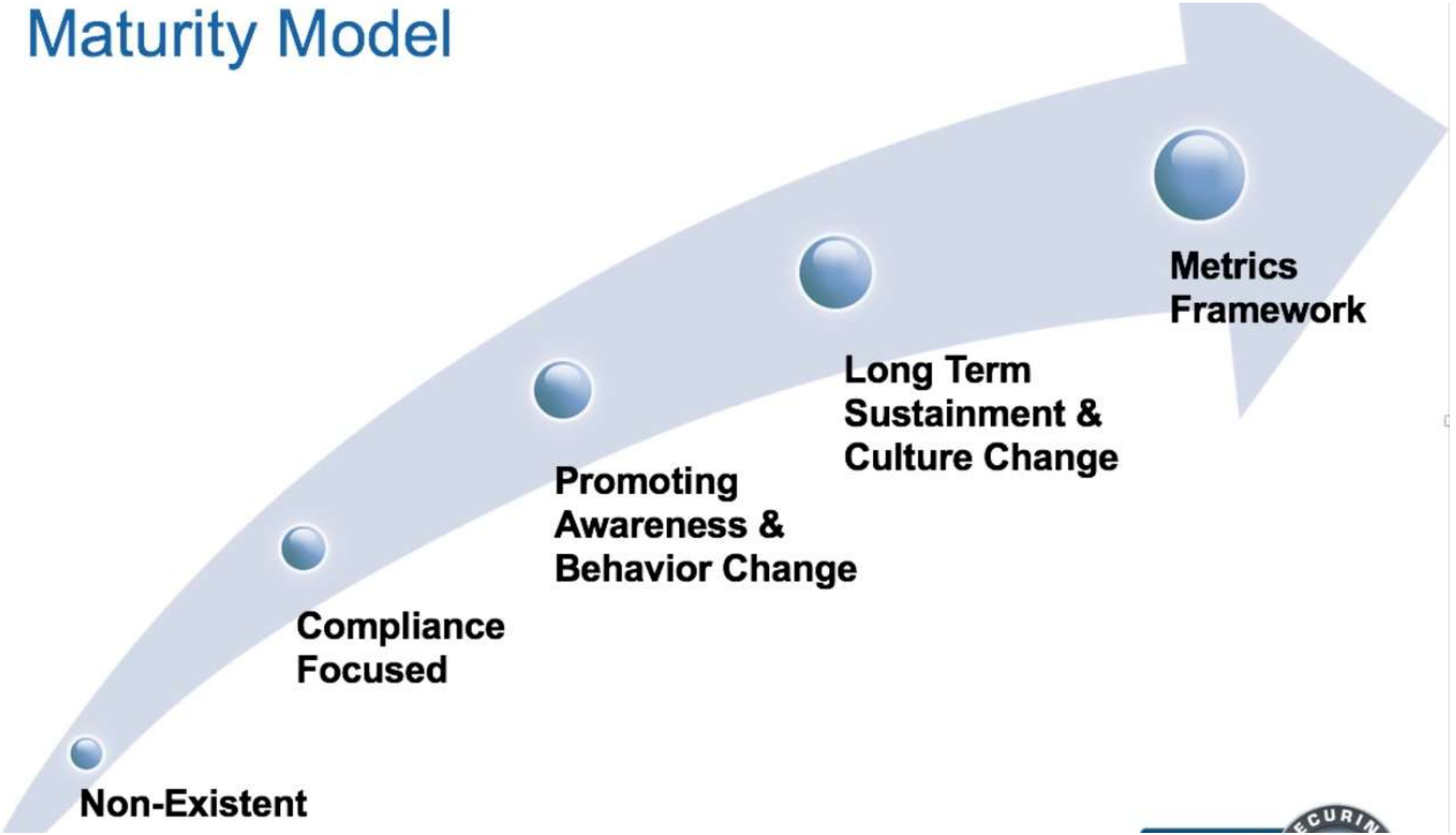
Documents followed by this icon may be downloaded at:
www.securingthehuman.org/resources/planning

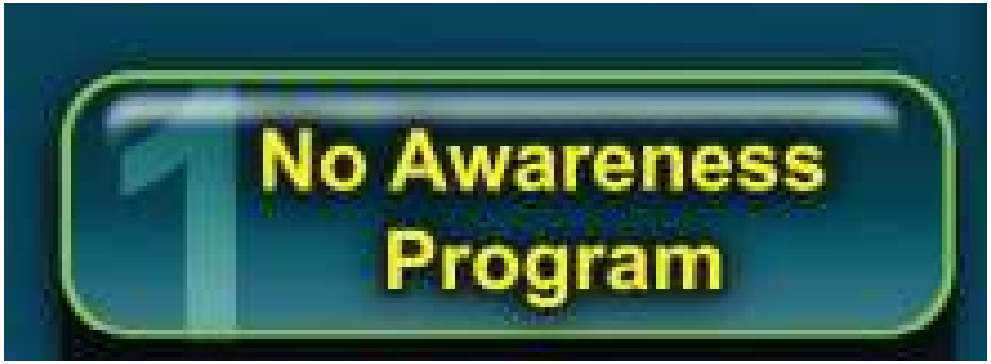
- Al igual que las computadoras, **las personas** almacenan, procesan y transfieren información.
- Sin embargo, muy poco se ha hecho para asegurar este "sistema operativo humano" (**HumanOS**).
- Como resultado, **las personas**, antes que la tecnología, son ahora el **vector de ataque principal**.
- La **concientización** en seguridad es una de las maneras más eficaces de abordar este problema.

- Esta **hoja de ruta** está diseñado para ayudar a su organización a construir, mantener y medir un programa de **concientización** de seguridad de alto impacto que reduce el riesgo, al cambiar el comportamiento de las personas y que también cumple con los requisitos legales, de cumplimiento y auditoría.

- Para utilizar esta hoja de ruta, primero identifique el **nivel de madurez** de su programa de **concientización** y defina a donde quiere llegar.

Maturity Model





- **El programa no existe**.

- Los empleados no tienen idea de que son un objetivo de ataque, no conocen o entienden las políticas de seguridad de la organización, y son fácilmente víctimas de ataques o de sus propios errores.

- Programa diseñado principalmente para cumplimiento específico (compliance) o auditoría.
- La capacitación es limitada ya sea en forma anual o ad-hoc.
- Los empleados no están seguros de cuales son las políticas organizativas, de su papel en la protección de los activos de la organización y cómo prevenir, identificar o informar un incidente de seguridad.

Cómo llegar

- Identificar estándares de cumplimiento o auditoría a la cual su organización debe adherirse.
- Identificar los requisitos de concienciación que requieren estos estándares, lo cual requerirá, probablemente, coordinación con los responsables de cumplimiento y/o auditoría.
- Desarrollar o contratar la capacitación para satisfacer esos requerimientos.
- Implementar capacitación de sensibilización de seguridad.
- Monitorear el proceso de capacitación.

Entregables

- Materiales de capacitación: videos, newsletters y presentaciones.
- Informe de quienes han completado satisfactoriamente la capacitación

Estándares que requieren ser parte de la concientización

- ISO / IEC 27002
- PCI DSS (Tarjetas de crédito)
- SOX
- GLBA (Gramm Leach Bliley Act - **Financieras**)
- FISMA (**Federal** Information Security Management Act)
- HIPAA (**Health** Insurance Portability and Accountability Act)
- CIP-004 (Critical Security Controls - SANS)
- Directiva de protección de datos de la UE

- Se identifican los temas de capacitación que tienen mayor impacto en apoyo a la misión de la organización y se centra en esos temas clave.
- El programa va más allá de una capacitación anual e incluye refuerzos continuos durante todo el año.
- El contenido se comunica de una manera atractiva y positiva que fomente el cambio de comportamiento en el trabajo, en el hogar y en tránsito.
- Como resultado, los empleados y los terceros comprenden y respetan las políticas de la organización, y activamente reconocen, previenen y reportan incidentes.

Cómo llegar (i)

- Comience identificando a los involucrados. Son las personas que son clave para el éxito de su programa. Una vez identificados, desarrolle y ejecute un plan para obtener su apoyo.
- Los métodos para obtener apoyo incluyen encuestas de riesgo humano, evaluaciones de concientización, análisis de causa/efecto de incidentes recientes, informes de la industria o análisis de costo-beneficio.
- Defina una línea de base del nivel de concienciación mediante una encuesta de riesgo humano o casos de phishing.
- Para obtener ejemplos adicionales, consulte la sección Métricas.

Cómo llegar (ii)

- Desarrolle un pre-proyecto que le dé autorización para comenzar el proceso de planificación.
- Defina las expectativas clave, incluyendo la identificación del gerente del proyecto, estimaciones de costos, alcance del programa, metas, hitos y supuestos.
- Obtenga la autorización correspondiente. Una vez aprobada, comience la planificación.
- Establezca un Comité de Conducción para ayudar en la planificación, ejecución y mantenimiento del programa de concientización. Este comité debería incluir entre 5 y 10 participantes voluntarios de diferentes departamentos o unidades de la organización.

Cómo llegar (iii)

Identifique a **QUIÉNES** está dirigido su programa. Diferentes roles pueden requerir entrenamiento diferente o adicional. Un primer programa incluirá un número grande de participantes, luego se desarrollarán programas más extendidos o específicos para grupos especiales.

- Identifique **QUÉ** va a comunicar a los diferentes grupos a los que apunta su programa. El objetivo es crear el contenido más corto posible que tenga el mayor impacto.
- Comience con un análisis de riesgo para identificar los más importantes para la organización, documente esos riesgos en una matriz y luego priorícelos.
- A continuación, seleccione los riesgos que abordará en su programa por prioridad. Estos riesgos definen los temas a capacitar.
- Luego cree un documento de Objetivos de Aprendizaje separado para cada tema e identifique los comportamientos clave que necesita cambiar para eliminar o mitigar esos riesgos.

Cómo llegar (iv)

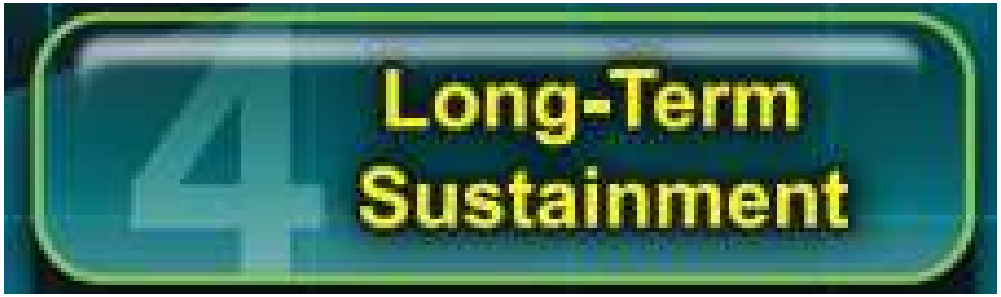
- Una vez que haya determinado **quiénes** son el objetivo de su programa y lo **qué** usted les transmitirá, determine **CÓMO** usted comunicará ese contenido.
- Para crear un programa atractivo, focalícese en cómo el destinatario habrá de beneficiarse de la capacitación y cómo la mayoría de las lecciones se aplican también a sus vidas personales.
- Hay dos categorías de capacitación: Primaria y de Refuerzo. La enseñanza primaria enseña nuevos contenidos y suele enseñarse anualmente o semestralmente y en el sitio o en línea. El entrenamiento de refuerzo se emplea durante el resto del año para reforzar los temas clave.
- Ejemplos comunes de entrenamiento de refuerzo incluyen boletines de noticias, carteles, podcasts, evaluaciones y blogs. Al enseñar un tema específico, consulte el documento de Objetivos de Aprendizaje para determinar qué contenido comunicar. De esta manera, independientemente de las diferentes maneras de comunicar un tema, el mensaje siempre será coherente.

Cómo llegar (v)

- Diseñe un plan de ejecución en coordinación con su Comité de Conducción.
- El plan debe comenzar con PORQUÉ se está lanzando un programa de concienciación de seguridad, sus objetivos y alcance general.
- A continuación, documente QUIÉNES, QUÉ y CÓMO.
- Incluya un cronograma que identifique la fecha de lanzamiento del programa, los hitos, los recursos críticos involucrados y cualquier otra información relevante.
- Haga que la dirección revise el plan. Una vez aprobado el plan, puede ejecutar su programa de concientización.
- Logre que el nivel más alto de la organización anuncie el programa ya sea a través del correo electrónico, publicación en un blog interno o video grabado.

Entregables

- Listado de involucrados y de los integrantes del Comité de Conducción
- Resultado del análisis de riesgo humano
- Pre-proyecto
- Matriz de contenidos
- Objetivos de aprendizaje de cada contenido
- Plan de ejecución



- El programa tiene procesos y recursos para un ciclo de vida de largo plazo , incluyendo (como mínimo) una revisión anual y actualización de contenidos de capacitación y métodos de comunicación.

- Como resultado, el programa va más allá del cambio de comportamientos y comienza a cambiar la cultura de la organización.

Cómo llegar (i)

- Identifique cuándo revisará su programa de concientización.
- Identifique nuevos o cambiantes tecnologías, amenazas, requisitos del negocio, de cumplimiento, estándares, etc. que deberían incluirse en la actualización anual.
- Realice una evaluación de su nivel de concientización y compárelo con la línea de base propuesta en la etapa 3.
- Realice una encuesta para conocer qué elementos gustaron más del programa, lo que necesita ser cambiado, qué tema encontraron más interesante y que comportamientos se logró cambiar.

Cómo llegar (ii)

- Realizar un análisis del riesgo humano y requerimientos de cumplimiento para determinar si hay nuevos temas que necesitan ser agregado o actualizado en su programa.
- Una vez que haya identificado los cambios proceder a revisar y actualizar el objetivo de aprendizaje para cada tema.
- Revise cómo han sido comunicados los contenidos, qué métodos han tenido el mayor impacto, y cuáles deben ser actualizados o eliminados.
- Realizar una revisión anual y actualización del presupuesto para reflejar los cambios en los objetivos.

Entregables

- Matriz que refleje los cambios que es necesario realizar con indicación de quién, cómo y cuándo deberá ser ejecutado.

- El programa tiene una estructura de métrica robusta para seguir el progreso y medir el impacto.

- Como resultado, el programa mejora continuamente y es capaz de demostrar el retorno sobre la inversión realizada.

Cómo llegar

- Hay dos categorías de métricas para programas de concientización: **cumplimiento e impacto**.
- Los de cumplimiento son utilizados por los auditores para verificar que el programa se haya llevado a cabo efectivamente.
- Las métricas de impacto miden el efecto que programa está teniendo en la conducta de los empleados y el efecto en la organización.
- Identificar los principales riesgos humanos que pretende mitigar e identifique las métricas que mejor miden el resultado.
- Documente cómo y cuándo tiene la intención de utilizar las métricas.
- Identifique a quién comunicar los resultados, cuando y cómo.
- Ejecute la aplicación de métricas.

Entregables y ejemplos

Matriz de métricas

- Ejemplos de métricas de cumplimiento del programa:
  - N° de personas que han completado el entrenamiento.
  - N° de empleados que han firmado La Política de Uso Aceptable.
  - N° de boletines o carteles repartidos.
  - N° de sesiones de capacitación in situ.
- Ejemplos de métricas de impacto del programa:
  - N° de empleados víctimas de simulaciones de phishing.
  - N° de documentos confidenciales en la papelera de
  - N° de sistemas infectados cada mes.
  - % de personas muestreadas con actitud positiva hacia la seguridad de la información.
  - % de personas que creen que sus compañeros de trabajo han compartido contraseñas con otros.