GUÍA DE IMPLEMENTACIÓN

Establecimiento de objetivos y planificación de su programa de concientización y capacitación sobre seguridad

Guía para la formación de una fuerza laboral con conciencia cibernética

Hubo un tiempo en el que los empleados se dedicaban a sus tareas diarias, ajenos a las posibles amenazas para su organización y para ellos mismos. Confiaban en que su equipo de seguridad informática tenía protegidos los datos, las redes, los dispositivos y los usuarios. En la actualidad, los empleados se convirtieron en objetivos de alto valor para los cibercriminales. Educar a los empleados sobre los riesgos de seguridad es fundamental. Un ataque exitoso, impulsado por un solo clic erróneo en un correo electrónico, puede cosechar millones de dólares para los criminales, y costar le a una organización millones de dólares en pérdida de confianza en la marca, multas de cumplimiento, ingresos, valor para los accionistas, y la lista continúa.

No se puede olvidar el factor humano en la ciberseguridad. La seguridad es ahora un asunto de todos.

Una solución de concientización y capacitación sobre seguridad debe contribuir a una cultura de seguridad global. Aplicar a la formación un enfoque de "casilla de verificación del cumplimiento" no fomenta una cultura de concientización, ni responde al panorama de amenazas en constante cambio. Es importante hacer de la concientización sobre ciberseguridad una parte integrada y continua de la cultura de trabajo de la organización. La concientización comienza con el individuo, y cada empleado tiene la responsabilidad de garantizar la seguridad de la información y los activos de una organización.

Pero ¿cómo involucrar a sus empleados y construir una cultura de conciencia cibernética?

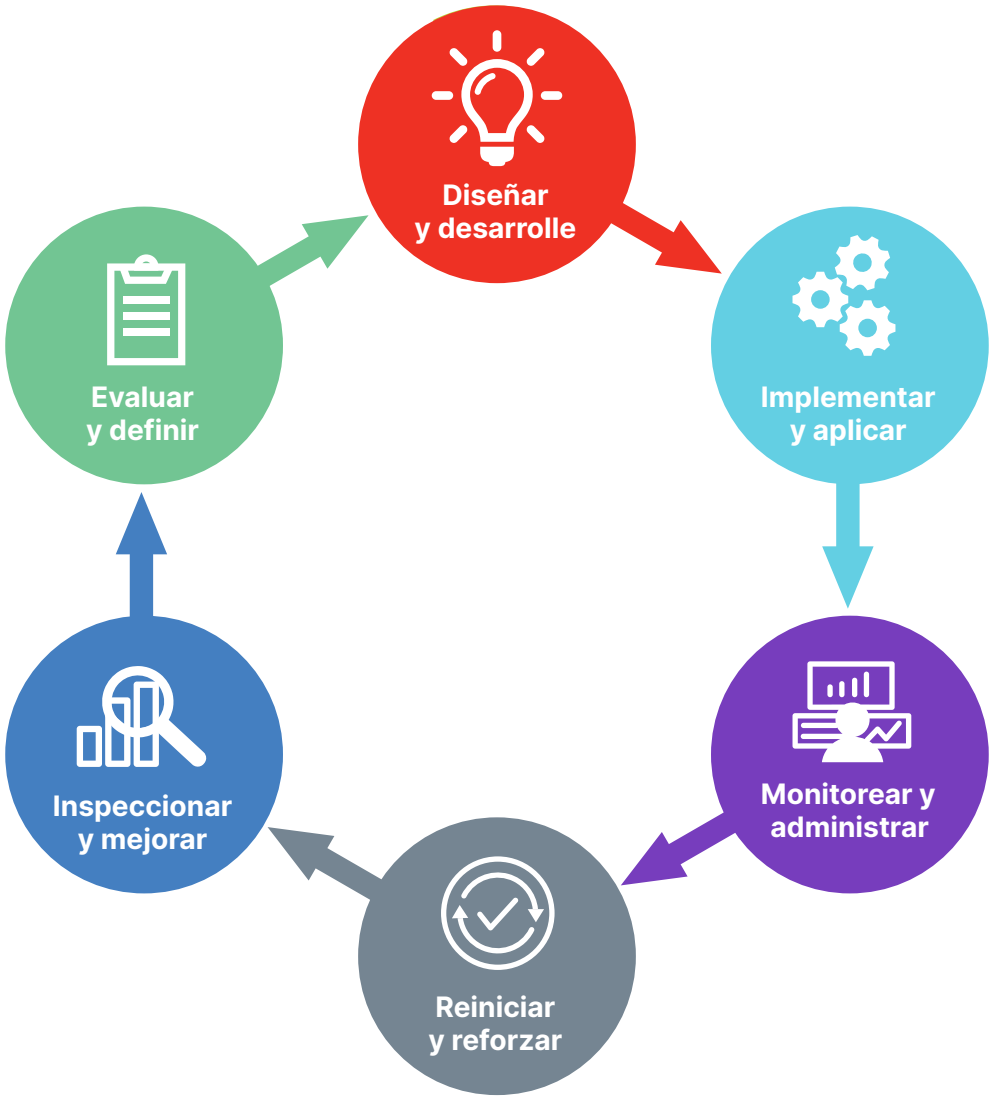

Figura 1: Un programa de concientización y capacitación sobre seguridad empieza por evaluar y definir las necesidades.

Evalúe y comprenda su línea de base: conozca sus riesgos

Antes de empezar, es esencial establecer una línea de base de los riesgos de seguridad actuales. Identificar los riesgos para su organización lo ayuda a desarrollar su plan y le permite evaluar si su programa de capacitación está marcando una diferencia en los hábitos de seguridad a lo largo del tiempo.

Un marco de ciberseguridad es un sistema de normas, lineamientos y mejores prácticas utilizadas para administrar los riesgos que surgen en el mundo digital. El marco suele coincidir con los objetivos de seguridad y se utiliza para desarrollar las políticas y procedimientos que definen las mejores prácticas que sigue una organización para administrar su riesgo de ciberseguridad.

Los gerentes deben preguntarse: "¿Qué resultados de ciberseguridad serían útiles para administrar el riesgo de ciberseguridad?" Hay una serie de marcos, como el Foro Económico Mundial (WEF): Principios y herramientas de ciberresiliencia para juntas directivas y el Marco de ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), a los que puede referirse cuando desarrolle un marco de seguridad alineado con su organización.

Riesgos para la seguridad de los empleados

Es una buena práctica probar los hábitos de seguridad de los empleados (o la falta de ellos) antes de inscribirlos en la capacitación. Las pruebas ayudan a establecer una línea de base para saber dónde están las áreas problemáticas y dónde centrar los esfuerzos de capacitación y refuerzo. Hay una serie de técnicas y herramientas que puede utilizar para conocer los hábitos de seguridad de sus empleados.

1. Comience practicando algunos ejercicios de simulación de suplantación de identidad. Registre los resultados. Incorpore la capacitación de seguimiento. Vuelva a practicar los ejercicios de simulación de suplantación de identidad. ¿Cuáles son los resultados ahora?
2. Monitoree los puntos de acceso y registre cualquier instancia de tailgating (empleados que les permiten a las personas entrar a los puntos de acceso sin pasar una credencial de acceso). Registre los resultados y vuelva a efectuar las pruebas en incrementos predeterminados.
3. Efectúe una revisión al azar, sin previo aviso, en los escritorios de su lugar de trabajo. Busque dispositivos cerrados con llave, gavetas, y documentos confidenciales. Registre los resultados y vuelva a efectuar las pruebas en incrementos predeterminados.
4. Emita una encuesta con preguntas clave.

Asegure el apoyo de los líderes y defina sus objetivos

Su equipo de liderazgo debe participar en el establecimiento de la misión y la directiva de su concientización y capacitación sobre seguridad. Cree un grupo de trabajo de liderazgo con funciones y responsabilidades asignadas, como la identificación de las metas y objetivos para la capacitación de los usuarios finales, la capacitación de los directivos, la adopción e incorporación de marcos de trabajo y los mandatos de cumplimiento.

Con el patrocinio de los ejecutivos, identifique las razones clave por las que su empresa quiere adoptar la concientización y capacitación sobre seguridad en toda la empresa. Comience por identificar sus objetivos. Piense por qué está implementando la capacitación y qué espera lograr al capacitar a sus empleados. Los objetivos típicos son: identificar las áreas problemáticas, aumentar los conocimientos de los empleados, crear cambios y reforzar las expectativas.

Asegúrese de que sus tareas y objetivos cuenten con la aprobación del presupuesto y la financiación.

Diseñe y desarrolle su plan de capacitación

Ahora que tiene el apoyo de los ejecutivos y una dirección claramente definida, puede empezar a desarrollar su plan de capacitación y concientización.

Estas son algunas de las preguntas que puede considerar en su plan:

- ¿Cómo será la cadencia de la capacitación? ¿Cómo administrará el proceso de incorporación, la capacitación anual, la evaluación continua y el servicio de capacitación en su conjunto?
- ¿Necesita una implementación gradual con un grupo de prueba piloto inicial? ¿Cómo va a captar las opiniones de los usuarios?
- ¿Necesita dirigirse a diferentes grupos en diferentes momentos con diferente material?

- ¿Qué temas deben abordarse en su organización para crear un programa que satisfaga sus necesidades organizativas específicas? Al elegir los temas, tenga en cuenta los comportamientos que desea integrar en las actividades cotidianas de sus empleados.
- ¿Necesita su organización un plan de comunicación centralizado, distribuido o ambos? (Consulte NIST 800-50, sección 3 para obtener lineamientos detallados).
- ¿Cómo va a distribuir todos los activos de comunicación (carteles, capturas de pantalla o cualquier otra cosa)?
- ¿Cómo va a comprobar los criterios de éxito?
- ¿Cómo se establecerán y ejecutarán las acciones de corrección?

Implementación: que todo el mundo participe

Ahora, está listo para implementar su programa de concientización de la seguridad y comunicárselo a los empleados. Le recomendamos que les comunique a sus empleados con anticipación que los está inscribiendo en la capacitación sobre concientización de la seguridad. También le recomendamos que establezca un plazo en el que sus empleados deben completar la capacitación y les envíe recordatorios. Comunique la importancia de la capacitación, su plan y su cronograma de capacitación a toda su organización. Conseguir que el equipo se comprometa es un paso clave para aumentar la concientización de la seguridad.

Seleccione los temas sobre los que desea que los miembros de su equipo aprendan más. Puede elegir los temas en función de sus pruebas de referencia, de los requerimientos empresariales o de los acontecimientos mundiales oportunos. Planifique el programa de capacitación. Establezca cuándo le distribuirá los módulos, activos y recursos a su equipo. Para mantener la seguridad en la mente, deben distribuirse con regularidad.

Monitoreo y administración

Administre el progreso de su programa de seguridad y concientización mediante el seguimiento del progreso de los empleados. ¿Quién recibió la capacitación? ¿Quién no y por qué? ¿En qué aspectos el rendimiento de los empleados es deficiente? ¿Observa algunas tendencias que puedan ayudarle a aumentar la adopción?

Además de monitorear el progreso de la capacitación de sus empleados, es probable que también quiera evaluar si, y cómo, los comportamientos de sus empleados respecto a la seguridad mejoran con el tiempo. Esto lo puede hacer estableciendo un ciclo que conste de una evaluación inicial de referencia, capacitación, reevaluación, y posiblemente, capacitación adicional para los empleados que no cumplieron con las expectativas.

A medida que revise su programa y descubra las brechas, tenga en cuenta lo siguiente para aplicar las medidas adecuadas:

- ¿Debe elevar las brechas a la dirección y debe tomar medidas sobre los rezagados?
- ¿Debe aumentar o disminuir la frecuencia de distribución de los módulos de capacitación?
- ¿Qué modificaciones debería hacer en la campaña de capacitación para cumplir los criterios de éxito?

Reinicie y refuerce el aprendizaje

A medida que monitoree su programa, considere ajustar o agregar nuevas campañas según sea necesario. Por ejemplo, si observa comportamientos erróneos o su organización está preocupada por una amenaza actual, considere la posibilidad de implementar módulos de nanoaprendizaje o microcapacitación como formación correctiva o refuerzo de enseñanzas clave. Distribuya hojas de sugerencias por correo electrónico o publíquelas en la intranet de su empresa, para que aparezcan en intervalos regulares.

Mantener la seguridad visible durante todo el año para ayudar a aumentar la conciencia de seguridad en toda su organización. Considere la posibilidad de ejecutar campañas relacionadas con diversos temas, como el Black Friday, la temporada navideña, etc.

Inspección y mejora

El objetivo clave de cualquier programa de capacitación sobre concientización de la seguridad es aumentar la sensibilidad y alterar, de manera positiva, el comportamiento del usuario para reducir los incidentes de seguridad de la información.

El objetivo de un plan de posimplementación es esforzarse por lograr una mejora continua. Monitorear el cumplimiento, ejecución de evaluaciones formales, y la recopilación de comentarios son las mejores prácticas que se pueden utilizar para construir la mejora continua dentro de su organización.

En la sección 6.2 de la Publicación especial 800-50 del NIST se describen las herramientas y tácticas para efectuar evaluaciones formales y recopilar comentarios. Estas incluyen:

- Diseño de una estrategia de comentarios
- Haga encuestas
- Cree informes de estado
- Haga entrevistas
- Haga observaciones
- Implemente grupos de enfoque
- Recopile y compare métricas (comparar a la línea de base)

La publicación también describe varios indicadores de éxito de los programas para la capacitación sobre concientización de la seguridad. Entre ellos se encuentran:

- La distribución de módulos y activos de concientización es compatible.
- El equipo ejecutivo está de acuerdo en enviar mensajes al personal sobre la seguridad informática.
- Las estadísticas indican una brecha cada vez menor entre la conciencia existente y las necesidades identificadas, un mayor porcentaje de usuarios expuestos a materiales de concientización, etc.
- Los gerentes participan en el proceso al inscribirse y completar sus módulos de concientización y alentar a otros a hacer lo mismo.
- Las contribuciones a la seguridad se reconocen mediante premios, concursos, etc.
- Los actores clave (directores, administradores de seguridad de la información, coordinadores de capacitación y otros) parecen estar motivados.

Utilice los indicadores de éxito para determinar si la implementación del programa fue exitosa. Si determina que no tuvo éxito, utilice los indicadores para determinar dónde puede hacer mejoras. La mejora continua y los cambios medibles en el comportamiento deben ser siempre los objetivos de cualquier programa exitoso de concientización sobre la seguridad de la información.

julio 29, 2022

1376805-0-0-ES