Plan de formación

La formación tiene la misión de capacitar al personal para prevenir, mitigar o dar respuesta a las posibles amenazas que puedan afectar al sistema.

La concienciación consiste en garantizar que todos los miembros de la organización están sensibilizados con la importancia de participar activamente en la seguridad de la información e involucrarlos a todos en la puesta en práctica de los distintos controles de seguridad, cada cual al nivel que le corresponda como responsable del uso o mantenimiento de los sistemas de información, mediante el cumplimiento de las políticas de seguridad establecidas.

Este plan de formación debe tener en cuenta:

- Todo el personal debe recibir una formación y concienciación iniciales:
- La formación estará más orientada al personal técnico que desempeñe funciones directas sobre la seguridad, la configuración de sistemas, el tratamiento de la información, la gestión de incidentes, etc. El resto del personal recibirá una formación básica en técnicas de ciberseguridad y buenas prácticas en el puesto de trabajo.

- La concienciación se hará de manera general para todo el personal de la organización.
- La concienciación y la formación deben refrescarse y actualizarse regularmente:
- La formación debe actualizarse cada vez que se producen cambios en el sistema, ya sean de hardware, software o instalaciones de red, entre otros.
- Es importante refrescar la normativa de seguridad relativa al uso responsable de los sistemas aunque no se produzcan incidentes.

poder crear un programa de formación adecuado. De lo contrario se corre el riesgo de que la formación sea insuficiente o excesiva.

- **Roles y responsabilidades**: La formación debe estar adaptada a los roles y responsabilidades de cada persona, en función de aspectos como:
  - El nivel de acceso a los sistemas e información.
  - Procesos que realizan.
  - Personas con las que interactúan.
  - Ubicaciones en las que trabajan.
- **Tipos de activos**: La formación debe estar adaptada a los activos que maneja cada persona, por ejemplo:
  - Datos financieros.
  - Datos de RRHH.
  - Datos de salud.
  - Proyectos de infraestructuras críticas.
  - Datos personales de clientes, proveedores o de la propia organización.

Servicios disponibles

Dependiendo de que servicios use la organización también tendremos que tenerlos en cuenta en el plan de formación:

- **Web**: En muchas ocasiones la web no es solo un frontend para los clientes, sino que también es un frontend para los empleados. Por lo tanto, es importante que los empleados conozcan los riesgos asociados a la web y cómo protegerse.
- **Almacenamiento en la nube**: Es fácil no cumplir con la normativa legal de protección de datos si no se tiene en cuenta que los datos están en la nube.

- **Correo electrónico**: Es el principal vector de ataque. Es importante que los empleados sepan cómo identificar correos maliciosos y cómo actuar en caso de recibir uno.
- **Redes sociales**: Es importante que los empleados sepan cómo proteger su privacidad y la de la empresa en las redes sociales. La reputación de la empresa puede verse afectada por lo que se comparte en redes sociales.

Políticas de empresa

Otro aspecto importante, por ejemplo:

- Trabajo presencial o remoto.
- Uso de dispositivos personales (BYOD).
- Uso de dispositivos corporativos, como portátiles, móviles, tablets, etc.
- Uso de redes corporativas o públicas.
- Uso de aplicaciones corporativas o públicas.
- Uso de servicios en la nube.
- Uso de correo electrónico.
- Uso de redes sociales.
- Uso de mensajería instantánea.
- Uso de servicios de videoconferencia.

◇

Otros

Es difícil que un solo plan de formación cubra todas las necesidades de una organización. Por eso, es importante que se haga una evaluación de las necesidades de formación de la organización y se diseñe un plan de formación a medida.

Algunos aspectos adicionales que pueden ser importantes a tener en cuenta:

- Tamaño de la organización.
- Ámbito de negocio.
- Horarios y turnos de trabajo.
- Localización y número de sedes.

Contenidos de la formación

Algunos de los contenidos básicos a cubrir:

- **Utilización de contraseñas seguras y sistemas de doble verificación**: instruir a los empleados sobre el uso de las contraseñas dificultará accesos no autorizados.
- **Phishing**: reconocer correos electrónicos sospechosos que pueden llevar a revelar credenciales de acceso u otros datos sensibles.
- **Peligros de las descargas y utilización de software no autorizado**: no se debe permitir software no autorizado en dispositivos corporativos. Este software descargado de fuentes no confiables a menudo puede contener malware, virus o spyware ocultos.

- **Uso apropiado de internet**: definir qué está permitido y qué no a la hora de utilizar la red y establecer conexiones en internet para que las actividades realizadas dentro del entorno laboral se hagan de una manera segura.
- **Ingeniería social**: establecer pautas sobre cómo evitar caer en la manipulación de los ciberdelincuentes que intentarán que les proporcionen información confidencial o personal o que hagan algo que les ayude a acceder a los sistemas de la organización. En muchos casos la ingeniería social estará asociada con el phishing.
- **Uso de dispositivos de almacenamiento externo**: pueden presentar ciertos riesgos y peligros, como propagación del malware o perdida o robo de datos, ya que son altamente susceptibles de sufrir daños o extraviarse.

◇

- **Políticas de trabajo remoto**: el trabajo remoto se ha vuelto cada vez más común y los empleados deben saber cómo hacer para que los accesos sean seguros y mantener así la integridad de los datos y los sistemas.
- **Redes inalámbricas**: relacionado con el punto anterior, el trabajo remoto permite a los empleados trabajar desde cualquier lugar, incluso desde localizaciones con redes wifi públicas que pueden ser vulnerables al acceso no autorizado por parte de atacantes si no están protegidas adecuadamente.
- **Actualización del software**: las actualizaciones de software a menudo incluyen parches de seguridad que solventan vulnerabilidades y protegen contra amenazas potenciales, por lo que la actualización periódica del software ayuda a garantizar que las medidas de seguridad estén al día para proteger mejor los sistemas contra posibles ataques.

- **Copias de seguridad**: es esencial para la continuidad del negocio formar a los empleados sobre las copias de seguridad periódicas de los datos críticos y sobre el proceso de restauración para garantizar que los datos se puedan recuperar durante un incidente de seguridad.
- **Notificación de incidentes**: los empleados deben ser conscientes de la importancia de notificar cualquier hecho o actividad sospechosa de la que tengan conocimiento. Esta información permite a los equipos de seguridad responder de manera rápida y efectiva, ayudando a minimizar el impacto del incidente, evitando daños mayores. El plan de concienciación debe asegurar que los empleados conocen los canales de notificación.

- **Ley de protección de datos**: incluir también educación sobre los aspectos legales de las violaciones de datos, incluidas las sanciones por incumplimiento de las leyes de protección de datos.
- **Política de mesa limpia**: consiste en tener la mesa de trabajo despejada, solo con lo necesario para trabajar en ese momento y no dejar a la vista información sensible, sobre todo cuando el empleado se ausenta del puesto de trabajo, aunque sea por poco tiempo (Figura 1.10).

Elaboración del plan de formación y concienciación

Roles incluidos en el plan de formación y concienciación

Cada empleado tiene un papel que desempeñar para garantizar que la infraestructura de información de la organización permanezca segura, por lo que es importante establecer en el plan los diferentes grupos de empleados, departamentos o roles de usuarios junto con sus funciones y responsabilidades.

◇

En ocasiones, es necesario hacer subdivisiones de los grupos debido a características geográficas, horarias o logísticas. Por ejemplo:

- Si la organización tiene personal comercial trabajando en remoto y personal comercial trabajando en oficina, dentro del grupo comercial puede ser necesario crear un subgrupo «comercial remoto» y otro «comercial oficina» para en el primer grupo hacer formaciones online y para el segundo formación in situ.
- Si la empresa tiene turnos de mañana y tarde para el personal técnico, unificar su formación puede ser complicado; en este caso, también podría hacerse una subdivisión de este grupo para impartir formaciones en distintos tramos horarios que se adapten al horario laboral.

Contenidos

Notificar a los miembros del personal sobre la situación de seguridad actual de la organización es el primer paso para involucrarlos en la educación sobre ciberseguridad.

Seguidamente se debe formar y concienciar a los empleados sobre los diferentes tipos de amenazas que pueden encontrar durante la realización de sus funciones y las buenas prácticas.

Es esencial adaptar los contenidos lo mejor posible a las necesidades de la organización y a los roles de los empleados. Por ejemplo:

- Los empleados de RRHH pueden necesitar formación específica sobre cómo proteger los datos de los empleados en el software que usan.
- Los empleados de TI pueden necesitar formación sobre cómo proteger los sistemas de información
- Los empleados de ventas necesitará formación sobre cómo proteger los datos de los clientes en el software específico que usan.

- En general, formación sobre phishing, contraseñas seguras, uso de dispositivos de almacenamiento externo, uso de redes inalámbricas, actualización del software, copias de seguridad, notificación de incidentes y ley de protección de datos.
- El personal técnico se le dará una formación más avanzada sobre las últimas amenazas, administración de firewalls, prácticas de codificación segura, cifrado, uso de VPN y estrategias de respuesta a incidentes.

Evaluación

Cada plan de formación y concienciación debe ser evaluado para asegurarse de que cumple con los objetivos establecidos.

Esta evaluación puede incluir pruebas para examinar la adquisición de conocimientos, encuestas de opinión sobre la formación, simulaciones de ataques, etc.

Pruebas y encuestas

Para la realización de pruebas y encuestas puedes usar Google Forms, SurveyMonkey, Typeform o Microsoft Forms.

Campañas de phishing

Las campañas de phishing son una forma efectiva de evaluar la concienciación de los empleados sobre los correos electrónicos maliciosos.

Con kali linux puedes usar GoPhish para realizar campañas de phishing.

◇

GoPhish

GoPhish es una herramienta de phishing de código abierto que permite a los equipos de seguridad realizar campañas de phishing de manera sencilla y efectiva.

Para usarlo lanza el comando `gophish` en la terminal.

Una vez lanzado, abre un navegador y accede a `http://localhost:3333`.

Simulaciones de ataques

Puedes usar `Metasploit` para realizar simulaciones de ataques a la red de la organización, `hydra` para realizar ataques de fuerza bruta a contraseñas, `nmap` para escanear la red y `Wireshark` para analizar el tráfico de red y compronbar si hay fugas de información.

Materiales de formación

Debemos saber crear materiales de formación efectivos. Algunas recomendaciones:

- **Simplicidad**: los materiales de formación deben ser fáciles de entender y no contener información innecesaria.
- **Interactividad**: si pueden ser interactivos mejor, ya que esto aumenta la retención de la información.
- **Multimedia**: los materiales de formación pueden ser más efectivos si contienen imágenes, vídeos, animaciones, etc.

Tipos de materiales

INCIBE® propone en su kit de concienciación diversos tipos de materiales, como son:

- Pósteres/carteles: estos deben tener un título breve y atractivo que proporcione una comunicación inmediata y una imagen impactante que atraiga al destinatario.
- Presentaciones multimedia: se utilizarán principalmente para las jornadas y formaciones de un tema específico.
- Trípticos: un tríptico es un material de comunicación muy versátil que une la atracción inicial de un póster en su portada y en su interior sintetiza la información que se puede encontrar en una presentación. Además, en su contraportada suele incluir información de contacto.

- Encuestas de satisfacción: consultas a los empleados para recopilar comentarios sobre el plan de formación y concienciación.
- Ataques simulados de malware: utiliza diferentes métodos de entrenamiento, incluida la simulación de ataques. Esto puede ayudar a los empleados a comprender cómo podría ser un ataque real y cómo deberían responder.
- Campañas de simulación de phishing: envío de correos intentando que los empleados «piquen» en la estafa, para probar su conocimiento y preparación ante el phishing.

Una vez recopilados los materiales que se van a utilizar para el plan de formación y concienciación, estos pueden distribuirse a través de diversos canales como correo electrónico, portales de la intranet corporativa, vídeos en las salas comunes, y carteles y trípticos repartidos por las instalaciones.

La ciberseguridad es un proceso global tanto del ámbito corporativo como del doméstico; quien no navega por páginas inseguras en su casa previsiblemente tampoco lo hará en su puesto de trabajo, por lo que además de estos materiales es interesante ofrecer a los empleados recursos para el autoaprendizaje en ciberseguridad como cursos sobre ciberseguridad personal.

Una forma de auditar el cumplimiento y la efectividad de las medidas de seguridad y de la formación y concienciación de los empleados es establecer métricas o indicadores de logro. Algunas de estas métricas podrían ser:

- Número de veces que se clica en un enlace de un correo de phishing.
- Frecuencia con la que se cae en un engaño de ingeniería social.
- Número de denuncias sobre posibles incidentes.
- Tasa de participacion en las jornadas y cursos de formación.

- Resultados de las pruebas de los empleados sobre los conocimientos impartidos.
- callicaciones de los certificados oficiales del personal técnico.
- Comparativa del número de incidentes acaecidos antes y después de la puesta en marcha del plan.
- Número de reinstalaciones de sistemas debido a infecciones por malware.

Además de establecer estos indicadores, es importante acotar qué resultados se consideran un logro y cuáles no, ya que estos límites pueden variar según los objetivos y las medidas implementadas. Y en caso de que el logro no sea el esperado habrá que establecer qué medidas se van a tomar al respecto. Otra opción interesante es establecer recompensas o reconocimientos cuando los logros se han alcanzado o se han superado las expectativas.

Por ejemplo, si más del 50% de los empleados hace clic en correos electrónicos de phishing simulados puede indicar que es necesario revisar el programa. Por el contrario, si solo un pequeño porcentaje «pica el anzuelo», puede que solo sea necesario un repaso más personalizado de los conocimientos abordados en el plan de concienciación.