CURSO: GOBERNANZA Y GESTIÓN ESTRATÉGICA DE LA SEGURIDAD DE LA INFORMACIÓN

Unidad 5: Cultura de Ciberseguridad

Patricia Prandini y Raúl Saroka
DOCENTES

Índice

- Contexto
- Qué es la cultura organizacional
- Qué es una cultura de la ciberseguridad
- Acciones que favorecen una cultura de ciberseguridad
- Concientización, capacitación y formación

Que es cultura

1. Cultivo.
2. Conjunto de conocimientos que permite a alguien desarrollar su juicio crítico.
3. **Conjunto de modos de vida y costumbres, conocimientos y grado de desarrollo artístico, científico, industrial, en una época, grupo social, etc.**
4. Culto religioso.

Fuente: RAE

Cultura de ciberseguridad

La **cultura de ciberseguridad** es el conjunto de valores, comportamientos y prácticas adoptadas por una organización y sus integrantes con el objetivo de proteger la integridad, confidencialidad y disponibilidad de sus activos de información.

Refiere a la actitud y comportamiento de una organización o comunidad hacia la protección de la información que gestionan. Esto incluye la capacitación para reconocer los riesgos de seguridad, el uso seguro del software y la implementación de buenas prácticas en el uso de tecnología.

Beneficios de una Cultura de ciberseguridad

Menor riesgo de sufrir incidentes de ciberseguridad

Mayor conciencia sobre el uso responsable de las TI por parte de empleados y usuarios

Mayor rapidez y efectividad ante la ocurrencia de incidentes de ciberseguridad

Ahorro de costos a largo plazo al prevenir crisis costosas y pérdida de datos

Cultura de ciberseguridad

- Entrado este siglo, empieza a aparecer evidencia de la importancia de la cultura de la ciberseguridad al momento de mantener un nivel adecuado de seguridad de la información en la organización. (Ruighaver et al., 2007).

- Es clave el compromiso de las autoridades, la concientización y el entrenamiento, el involucramiento de todo el personal, la comunicación y la experiencia.

Cultura de ciberseguridad

Algunas consideraciones:

- Es importante saber que elementos crean la cultura, o los factores que tienen influencia en ella, para comprender de manera efectiva el comportamiento humano y por qué los empleados actúan de una manera determinada frente a la ciberseguridad.
- Entender los valores que dirigen las acciones de los individuos puede contribuir a un mayor entendimiento de cuestiones vinculadas al cumplimiento de políticas de la seguridad de la información. (Hedström et al., 2011)

Cultura de ciberseguridad

Algunas consideraciones - 2:

- La cultura de ciberseguridad no es solo responsabilidad del área de TI.
- Las personas pueden ser una amenaza o una vulnerabilidad para la confidencialidad, integridad y disponibilidad de la información.
- Los proyectos de aseguramiento de la información muchas veces no tienen en cuenta el factor humano, ignorando que la ciberseguridad **depende** de ellos.
- El gobierno y la gestión de la ciberseguridad es básicamente un desafío humano.

Cultura de ciberseguridad

Algunas consideraciones – 3:

- El incumplimiento es generalmente, el resultado de valores incongruentes, resultantes de lo que dicen las políticas y de lo que efectivamente se aplica al trabajo.
- Una cultura de la ciberseguridad madura se asocia a la puesta en valor de la concientización en seguridad y la percepción del riesgo y de la criticidad de los cambios en las amenazas.
- Las organizaciones pueden entender que el personal representa un riesgo o bien considerar que son un activo que empoderado, contribuye a la protección de la información.

Cultura de ciberseguridad

Algunas consideraciones – 4:

- Cualquier intento de cambiar o mejorar la ciberseguridad debe considerar los aspectos culturales de la organización.
- La cultura puede ser cambiada o modificada.
- Se la entiende como una parte de la cultura organizacional.

La cultura organizacional es el conjunto de presunciones básicas y tácitas sobre en que es o debería ser el mundo, entendimiento que es compartido por un grupo de personas y que determina sus percepciones, pensamientos, sentimientos y su comportamiento.

Fuente: Schein

Cultura organizacional

Tres niveles:

- Presunciones básicas, o creencias sobre la realidad vinculados a la naturaleza humana (organizacional vs. técnica, dinámica o estática, controles técnicos o empoderamiento de empleados, etc.)
- Valores relacionados con los principios, filosofías, objetivos y estandares sociales, (congruencia de objetivos, responsabilidad compartida, involucramiento y comunicación, etc.)
- Artefactos, es decir, resultados visibles y tangibles de las actividades que se desarrollan en base a valores y suposisicones (apoyo de autoridades, gestion del conocimiento, procesos de concientización y entrenamiento, etc.)

Acciones que favorecen la ciberseguridad

- Respaldo del directorio y del nivel gerencial: su apoyo es crucial
  - Voluntad de invertir en actividades de ciberseguridad
  - Organización de la función de ciberseguridad
  - Seguimiento de las tareas de ciberseguridad
  - Formulación e implementación de políticas de ciberseguridad
- Políticas de ciberseguridad, que demuestran la intención de las autoridades y proveen una guía
  - Deben reflejar un balance entre las expectativas de los empleados y de la gerencia
  - Se espera que sean congruentes con el modo de trabajo, que fomenten la ausencia de conflictos y que clarifiquen responsabilidades y expectativas

Acciones que favorecen la ciberseguridad

- Concientización y entrenamiento del personal
  - Uno de los aspectos centrales de la cultura de ciberseguridad es el conocimiento.
  - Existen 5 factores que influyen en el comportamiento del personal respecto a la ciberseguridad:
    - Falta de motivación
    - Escasas o inexistentes instancias de concientización
    - Creencias imprecisas e inadecuadas sobre el riesgo,
    - Comportamiento arriesgado
    - Uso inadecuado de la tecnología.
  - Los usuarios suelen ser apáticos y creer que es poco lo que pueden hacer frente a los problemas de ciberseguridad.

Acciones que favorecen la ciberseguridad

- Concientización y entrenamiento del personal
  - Debe tener en cuenta el contexto.
  - No se debe asumir que el empleado promedio tiene el conocimiento necesario para llevar adelante su tarea de modo seguro.
  - Roles diferentes tienen distintas necesidades de concientización.
  - Se ha comprobado que cualquier proceso de concientización que destaque el rol transformador de las autoridades, influye positivamente en la organización ya que empodera a los tomadores de decisión para explicar al personal de todos los niveles y persuadirlo sobre la relevancia de la ciberseguridad.
  - Muchos programas de concientización fallan porque no son atractivos y no invitan al personal a pensar cómo aplicar mecanismos de seguridad.
  - Es un esfuerzo continuo y parte de una campaña de concientización.

Acciones que favorecen la ciberseguridad

- Involucramiento y comunicación, en todos los niveles, tanto horizontal como verticalmente
  - La motivación debe promover la reflexión continua sobre el comportamiento de cada uno, la manera en que esto influye en la ciberseguridad y qué pueden hacer para mejorarla.
  - Se ha demostrado que los empleados tienen el potencial para contribuir positivamente a un ambiente más seguro si su participación es incentivada y se promueve la proactividad.
  - Los CISO deben adoptar una postura más participativa, con una comunicación efectiva con sus empleados en ambos sentidos y mejores instancias de negociación e involucramiento, que eviten el "*nosotros y ellos*".
  - Se debe formentar en determinados usuarios el sentido de propiedad o responsabilidad.
  - Compartir conocimientos sobre ciberseguridad resulta esencial.

Acciones que favorecen la ciberseguridad

- Aprendizaje a partir de la experiencia
  - El monitoreo de determinados indicadores y procesos para validar o mejorar un resultado es importante a los fines de la seguridad.
  - La auditoría es un buen ejemplo de este tipo de mecanismos, que pueden aportar valor en los procesos de concientización. El foco no debe estar en pasar la auditoría sino en alcanzar los objetivos fijados.
  - También puede ayudar el uso de modelos de madurez.
  - A menudo los sistemas de reporte de incidentes fallan al reconocer solo el componente técnico.

Existen varias similitudes entre una cultura de ciberseguridad y una de seguridad física pero la influencia de aspectos organizacionales y del contexto es más relevante en la de ciberseguridad. (Reeggard et al, 2019)

Despliegue de la Ciberseguridad

Tecnología

Procesos

Personas

Factor clave

Ciberseguridad

Educar

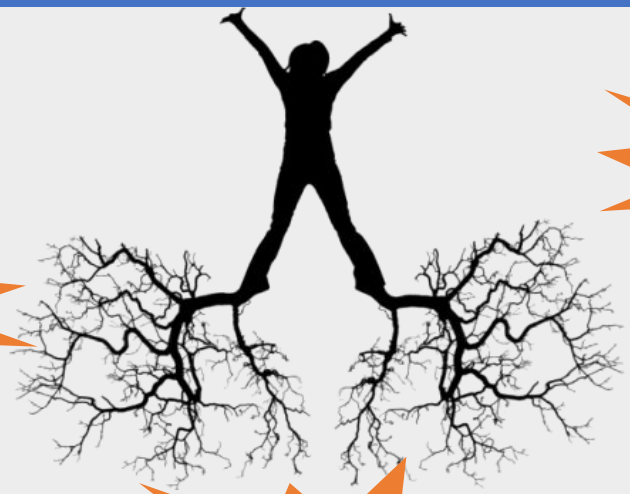
Entrenar

Concientizar

La ciberseguridad depende fuertemente del comportamiento de las personas

Contexto

Las personas pueden ser ORIGEN, BLANCO O MEDIO de la inseguridad de la información.



- Resistencia a cumplir
- Apatía
- Inconsciencia
- Disvalores
- Ignorancia
- …….

Concientización, capacitación y formación

- **Concientizar**

  Propiciar un conocimiento reflexivo de las cosas y un cambio en el comportamiento de las personas

- **Capacitar/Entrenar**

  Conjunto de acciones dirigidas a poner una persona en condiciones de ejecutar satisfactoriamente una tarea en particular, proporcionándoles conocimientos

- **Formar profesionalmente/Educar**

  Conjunto de acciones dirigidas a habilitar aprendizajes

Concientización, capacitación y formación

	Concientización	Entrenamiento	Educación
Atributo	Qué	Cómo	Porqué
Nivel	Reflexivo	Conocimiento	Juicio
Objetivo	Reconocimiento	Habilidad	Comprensión
Método de enseñanza	Videos, posters, folletos, …	Clases, talleres, casos, …	Clases teóricas, Seminarios, …
Evaluación	Verdadero/Falso Opción múltiple	Solución de problemas	Ensayos
Impacto	Corto Plazo	Mediano Plazo	Largo Plazo

Fuente: NIST

Concientización

¿Quiénes?	Autoridades, empleados, proveedores, clientes, usuarios y terceros que tengan contacto con la información de la organización
¿Qué?	Deben comprender la importancia de la adopción de medidas para proteger la confidencialidad, integridad y disponibilidad de la información
¿Cómo?	Mensajes sencillos, breves, realistas, contundentes, que capten la atención

Protección de la información en la organización

La organización debe:

- **Capacitar al personal** desde su ingreso y en forma continua durante el desarrollo de sus tareas
- **Concientizar a los usuarios** para que respeten las Políticas de Seguridad y tengan un comportamiento responsable
- **Implementar adecuados mecanismos de control** en todas las etapas de vinculación de las personas con la organización e inclusive después de haberse desvinculado
- **Incluir responsabilidades en materia de seguridad** en los perfiles, contratos y acuerdos

A tener en cuenta

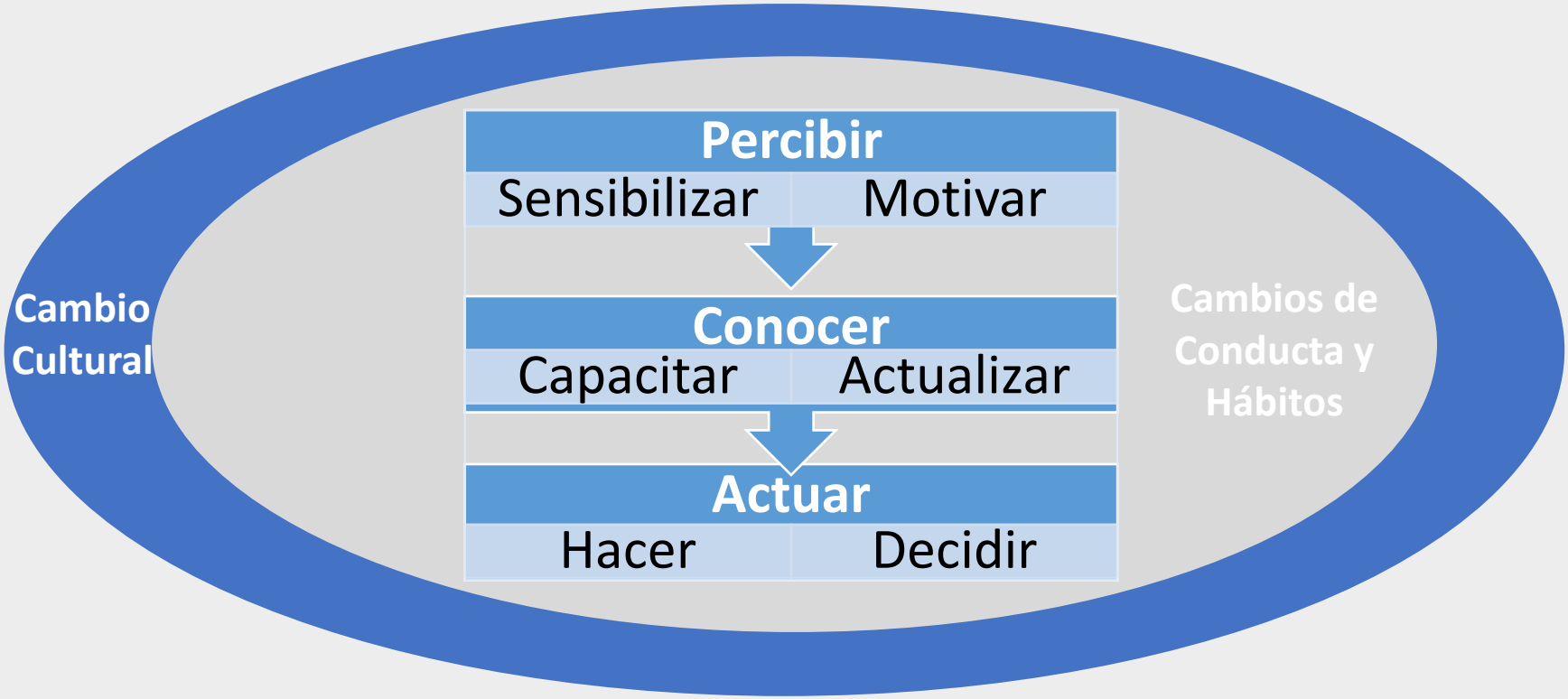
- El principal elemento para fortalecer la ciberseguridad en una organización es el empleado, que es quien accede y gestiona la información, ya sea creándola, procesándola, transmitiéndola o eliminándola.

- Una estrategia de limitación y prohibición es poco efectiva debido a que:
  - Se hacen más lentos los procesos de negocio
  - Provoca rechazo en los empleados y usuarios
  - Es muy difícil de controlar de modo eficiente, transparente y legal

LA SOLUCIÓN ES LA CONCIENTIZACIÓN DE LOS EMPLEADOS

Qué es Concientizar

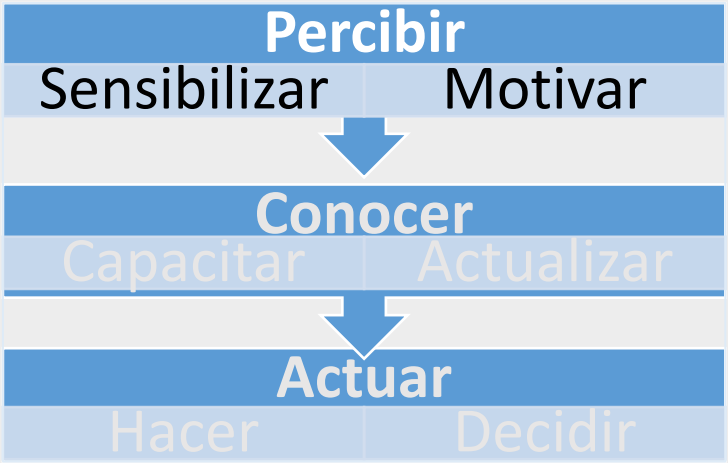
CONCIENCIA: Conocimiento que una persona tiene de sí misma y de su entorno.



Qué es Concientizar

Promover experiencias de dominio

Comprender el entorno que lo rodea



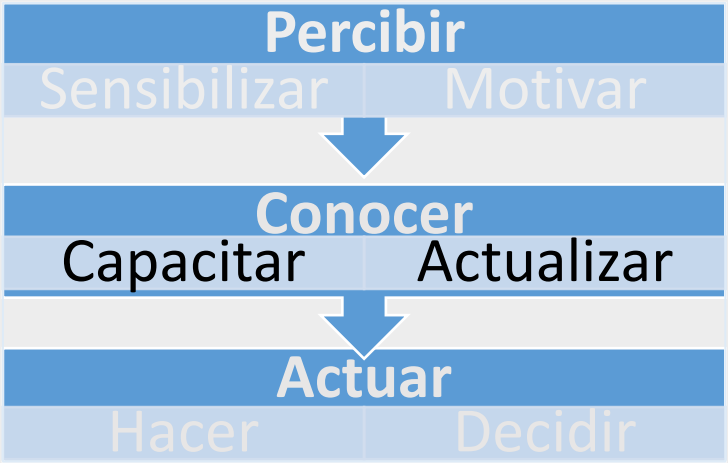
Descubrir las modificaciones externas que se provocan

Desarrollar la confianza en sí mismo

Qué es Concientizar

Favorecer la discriminación fantasía-realidad

Adquirir habilidades para hacer



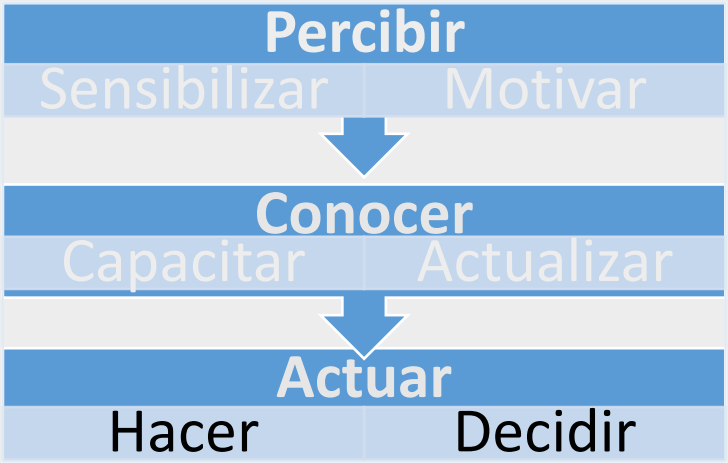
Estimular la atención y el pensamiento crítico

Habilitar una mejor interacción

Qué es Concientizar

Aumentar el nivel de alerta

Promover una actitud responsable



Estimular el autocontrol

Favorecer la colaboración

Ejemplo de programa de concientización

- Desarrollado por INCIBE (Instituto de Ciberseguridad de España) y actualizado en 2020
- Objetivo: ayudar a las empresas para mejorar la ciberseguridad en la organización a partir de las personas.
- Comprende recomendaciones y ejemplos de:
  - Recursos gráficos
  - Elementos interactivos
  - Una programación detallada

Ejemplo de programa de concientización

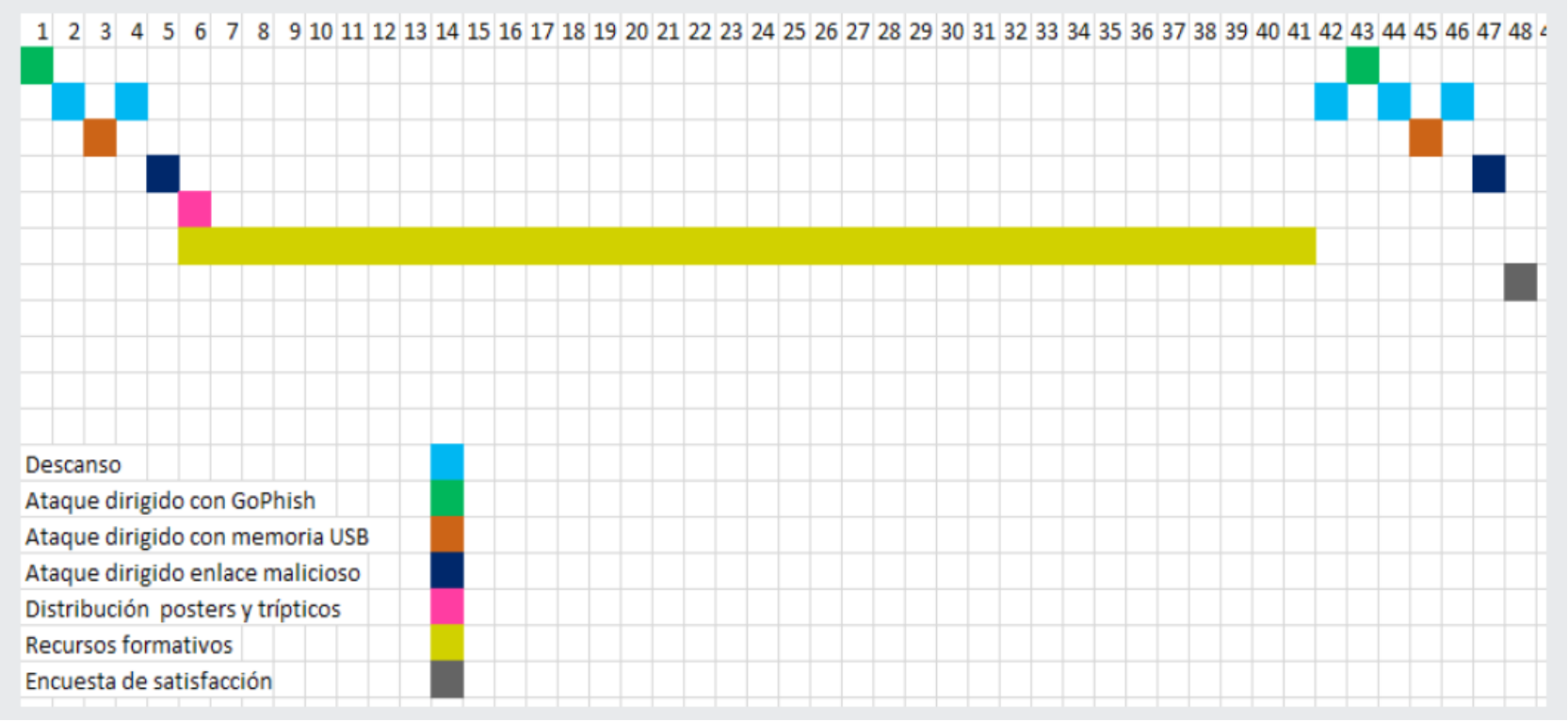
- **Ataques dirigidos** especialmente diseñados para evaluar el nivel concienciación en el uso del correo electrónico.
- **Posters**
- **Trípticos**
- **Recursos formativos,** que constan de 9 recursos formativos divididos en 6 temáticas distintas: la información, fraudes a través de correo electrónico, contraseñas, el puesto de trabajo, BYOD y teletrabajo y las redes sociales.
- **Encuesta de satisfacción**

Etapas del Kit de Concientización de INCIBE

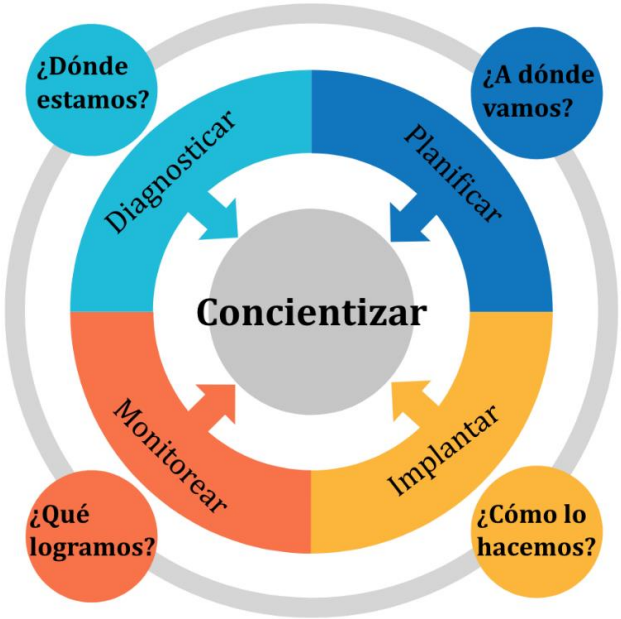
Propuesta de Cronograma orientativo

Tarea	Duración
Ataque dirigido con Gophish	5 días laborables
Descanso entre ataques	5 días laborables
Ataque dirigido memoria USB	5 días laborables
Descanso entre ataques	5 días laborables
Ataque enlace malicioso correo	5 días laborables
Distribución posters presentación y trípticos	1 día laborable
Recurso formativo	9 meses
Ataque dirigido con Gophish	5 días laborables
Descanso entre ataques	5 días laborables
Ataque dirigido memoria USB	5 días laborables
Descanso entre ataques	5 días laborables
Ataque enlace malicioso correo	5 días laborables
Encuesta de satisfacción	1 día laborable

Propuesta de Cronograma orientativo



Ejemplo de Plan de Trabajo



Fuente: Consultora GS Info

- Se construye el programa en base a la estrategia de negocio y las necesidades específicas de cada organización.
- Se establecen las prioridades de implantación, fechas, costes y recursos necesarios.
- Se monitorean los resultados en un proceso de mejora continua.

Ejemplo de Plan de Trabajo

- Se formula un **Plan de trabajo** para la campaña, que incluye un análisis de la seguridad de los sistemas y procedimientos de la organización, con objeto de que las acciones y medidas a ser implantadas sean acordes al escenario evaluado.

- Se formula un **diagnóstico** para determinar el contexto de la seguridad de la información, los temas de interés organizacional y las fortalezas y las debilidades a considerar.

- En la **planificación**, se determinan las actividades y servicios necesarios para remediar la situación identificada en el diagnóstico y las métricas que se utilizarán.

Fuente: Consultora GS Info

Ejemplo de Plan de Trabajo

- Posteriormente, se procede a la **implantación** que consiste en la puesta en marcha del plan de la campaña y se realizan las mediciones iniciales.

- Finalmente, se realiza un **monitoreo** para determinar la eficiencia y efectividad del programa y para definir acciones complementarias que optimicen los resultados y permitan definir próximas campañas.

Fuente: Consultora GS Info

CURSO: GOBERNANZA Y GESTIÓN ESTRATÉGICA DE LA SEGURIDAD DE LA INFORMACIÓN

Unidad 5: Cultura de Ciberseguridad

Patricia Prandini y Raúl Saroka
DOCENTES