Política de concienciación para gestión de amenazas internas

En esta política encuentra:

1. - Objetivos
2. - Alcance
3. - Directrices
4.- Cumplimiento de políticas

Objetivo:
Promover la concienciación en seguridad cibernética entre todos los empleados y proteger los activos digitales, la privacidad y la reputación de la organizacion contra posibles amenazas y riesgos cibernéticos.

ICS Instituto de Ciberseguridad
Prevención - Respuesta - Continuidad

contacto@iciberseguridad.io

MEX: +52 812-587-2530
ARG: +54 351 773 4308

www.iciberseguridad.io

Política

Contenido

Política

1. Objetivo

Promover la concienciación en seguridad cibernética entre todos los empleados de <Nombre_de_empresa>, con el fin de proteger los activos digitales, la privacidad y la reputación de <Nombre_de_empresa> contra posibles amenazas y riesgos cibernéticos.

2. Alcance

El alcance de esta política debe ser definida con base en las necesidades de la organización, entre esto se encuentra:

- Implementar a toda la organización
- Implementar a un área en especifico
- Implementar a las personas que hagan una actividad en particular
- Aquellas que por necesidad, la organización considere.

3. Directrices

La culturización de usuarios debe llevarse a cabo como un programa continuo para garantizar que la capacitación y el conocimiento no solo se brinden como una actividad anual, sino que se utilicen para mantener un alto nivel de conciencia de seguridad a diario

3.1- Crear el equipo de culturización

3.1.1. Para el desarrollo de un programa de culturización <Nombre_de_empresa> deberá definir el equipo que dará seguimiento a las actividades del programa, de forma enunciativa mas no limitativa:

- Desarrollo del programa
- Identificación de necesidades
- Mantenimiento del programa

3.1 Determinar roles y funciones

<Nombre_de_empresa> deberá considerar como mínimo, los siguientes roles deben abordarse en términos de cualquier necesidad de capacitación especial:

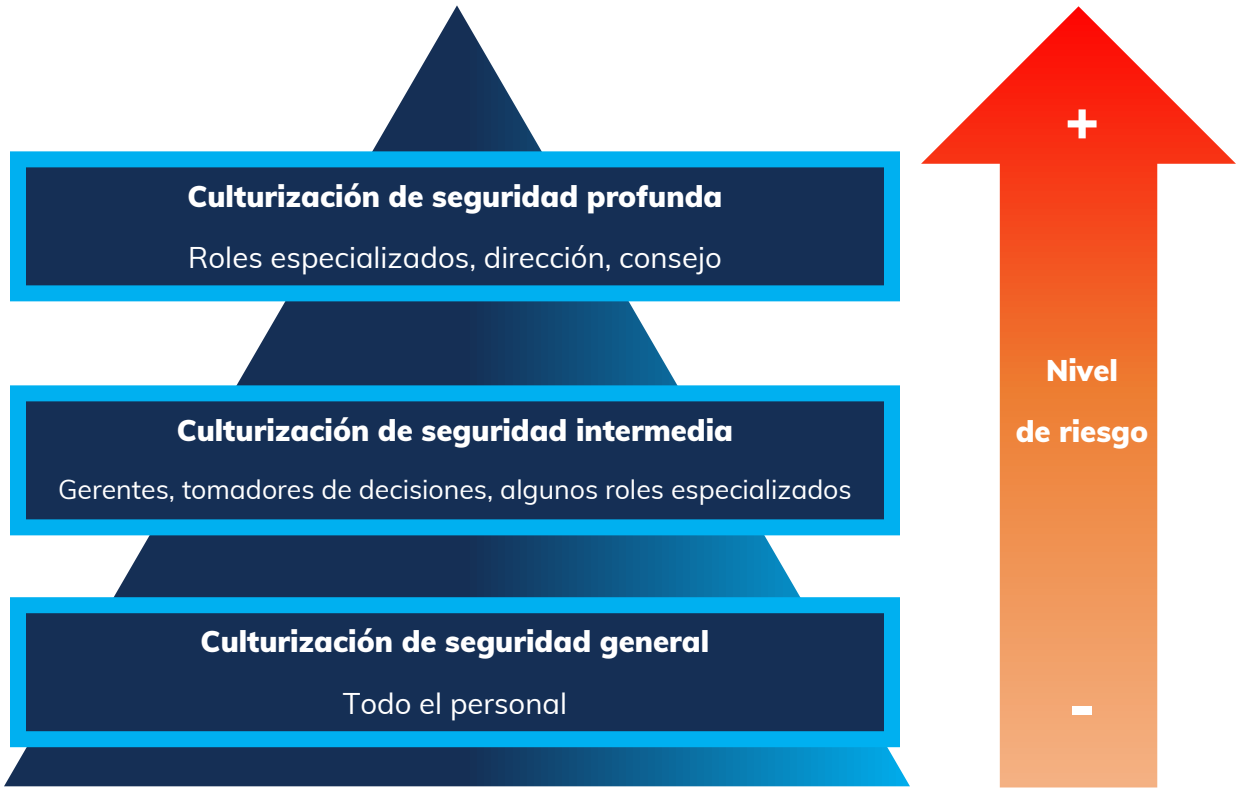
Rol	Actividades
Dirección	Los líderes de <Nombre_de_empresa> deben comprender completamente las directivas y las leyes que forman la base del programa de seguridad.
Propietarios de activos	Los propietarios de <Nombre_de_empresa> deben tener una amplia comprensión de las políticas de seguridad, así como los controles y requisitos aplicables de seguridad a los activos de los que son propietarios.
Personal	Todo el personal <Nombre_de_empresa> debe cumplir con las obligaciones de seguridad impuestas por la dirección.
Personal de RH	Deberá realizar las evaluaciones para la identificación de necesidades de capacitación en la organización.
Puesto organizacional	Actividades para realizar

3.3 Establecimiento de objetivos

<Nombre_de_empresa> deberá establecer los objetivos deseados para alcanzar un nivel mínimo de cultura en seguridad para el alcance fijado con anterioridad.

El programa de concientización sobre seguridad debe entregarse de manera que se ajuste a la cultura de de **<Nombre de su empresa>** y tenga el mayor impacto para el personal.

El siguiente diagrama muestra cómo la profundidad de la capacitación de concienciación debe aumentar a medida que aumenta el nivel de riesgo asociado con los diferentes roles (la asignación de roles es ajustable a la organización, este diagrama y política se crea acorde a una organización de 15 a 100 usuarios):



3.4 Apoyo directivo

La dirección y/o consejo de <Nombre_de_empresa> deberán ser consientes y proporcionar los recursos necesarios que permitan en diseño, despliegue y continuidad del plan de culturización.

<Nombre_de_rol> deberá informar sobre riesgos, objetivos y avances de estos a la dirección y/o consejo de <Nombre_de_empresa> con la finalidad de que se evalúe el nivel de cumplimiento y validar la permanencia de la estrategia.

3.5 Evaluar necesidades

<Nombre_de_empresa> deberá definir los mecanismos que permitan determinar las necesidades de capacitación, de forma enunciativa mas no limitativa a:

- **Entrevistas** con todos los grupos y organizaciones clave identificados
- **Revisión** de cualquier hallazgo y / o recomendación de los organismos de supervisión (por ejemplo, revisión / auditoría interna y programa de controles internos) o revisiones del programa con respecto al programa de seguridad de TI.
- **El análisis de eventos** (como ataques de denegación de servicio, desfiguración de sitios web, secuestro de sistemas utilizados en ataques posteriores, ataques de virus exitosos) podría indicar la necesidad de capacitación (o capacitación adicional) de grupos específicos de personas
- **El estudio de tendencias** identificadas por primera vez en publicaciones industriales, académicas o gubernamentales o por organizaciones de capacitación / educación. El uso de estos "principios

3.6 Desarrollo de una estrategia y plan de concientización y capacitación

<Nombre_de_empresa> deberá desarrollar, implementar y mantener su programa de capacitación y conciencia de seguridad que contemplen, de forma enunciativa mas no limitativa los siguientes elementos:

- Políticas nacionales y locales existentes que requieren conciencia.
- Cursos o materiales obligatorios (y si corresponde, opcionales) para cada público objetivo.
- Documentación, comentarios y evidencia de aprendizaje para cada aspecto del programa.
- Evaluación y actualización de material para cada aspecto del programa.
- Frecuencia en que cada público objetivo debe estar expuesto al contenido.

3.7. Calendarización para Implementación del programa de culturización

<Nombre_de_empresa> deberá desarrollar una calendarización del programa en seguridad de TI debe en los que se puedan identificar, de forma enunciativa mas no limitativa los siguientes puntos:

- Despliegue del contenido
- Evaluaciones de aprendizaje
- Presentación de informes a dirección
- Recomendaciones y actividades de mejora

3.8. Post implementación

<Nombre_de_empresa> deberá realizar evaluaciones que permitan identificar:

- El nivel de cumplimiento de los objetivos
- La efectividad general del programa
- La efectividad del contenido implementado
- La efectividad de los medios por los que se desplego el programa
- Cantidad de audiencia concientizada

3.9. Evaluación y retroalimentación

<Nombre_de_empresa> deberá contar con mecanismos de retroalimentación que permitan identificar:

- Dificultad de los mecanismos de despliegue de contenido
- Utilidad de la información
- Duración de la sesión
- Sugerencias de modificación.

Política

4. Cumplimiento de políticas

4.1 Excepciones

La dirección de <Nombre_de_empresa> deberá definir y aprobar cualquier excepción a la política.

4.2 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, que pueden incluir el despido.

Incluir en este apartado las actividades en las que incurriría en caso de incumplimiento de esta.

Elaborado por	**Nombre** Puesto
Revisado por	**Nombre** Puesto
Aprobado por	**Nombre** Puesto