PLAN DE COMUNICACIONES Y CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO

Tabla de contenido

1. OBJETIVO

El modelo de seguridad y privacidad de la información “MSPI” es un sistema de gestión vivo que debe ser atendido transversalmente en la **INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO**; con frecuencia los esfuerzos en este sentido se enfocan en tecnologías de información y en procesos de la Institución; sin embargo, ninguno de estos esfuerzos será suficiente para mantener un nivel adecuado de protección si existen brechas en la cultura, el comportamiento y la conciencia de las personas frente a la seguridad de la información, ciberseguridad y su responsabilidad en el cuidado de ésta.

Las iniciativas de toma de conciencia definidas en este documento buscan complementar la gestión del riesgo asociado al factor humano, impulsando en los empleados, estudiantes, contratistas, aprendices, practicantes o terceros y demás personas jurídicas o naturales que hacen uso de la información y de las tecnologías que la soportan en la IUE, la importancia de su protección y adoptar comportamientos responsables y seguros para su protección, convirtiéndose en la primera línea de defensa en la gestión de seguridad de información de la **INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO**.

2. ALCANCE

Este documento abarca la formulación de iniciativas tendientes a la adopción de hábitos y comportamientos adecuados frente a los activos de información institucionales por parte de los empleados, estudiantes, contratistas, aprendices, practicantes o terceros y demás personas jurídicas o naturales que hacen uso de la información y de las tecnologías que la soportan, lo que se traduce en la generación de una cultura organizacional que busca y propende por gestionar adecuadamente los riesgos de seguridad de la información y ciberseguridad de la institución.

La presente estrategia cubre:

- Los aspectos de seguridad de la información y ciberseguridad que serán abordados.
- Las iniciativas y los medios de comunicación que serán empleados para divulgar los mensajes de toma de conciencia.
- Calendario estimado para la realización de las iniciativas propuestas.

3. RESPONSABLES

- El rol responsable del mantenimiento y la mejora del presente documento es el **Encargado de la Ciberseguridad de la IUE**.
- La responsabilidad de la aprobación de lo dispuesto en este documento es del **comité de gestión y desempeño de la INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO.**

4. CONTENIDO

4.1. Temas

Entendiendo las debilidades de seguridad de la información asociados al factor humano que se han identificado en la institución, así como, considerando el contenido de las políticas de seguridad de la información vigentes; se han definido los siguientes aspectos que serán el foco de atención de las iniciativas propuestas:

- Políticas de seguridad de la IUE.
- Procesos y procedimientos del MSPI.
- Manejo de usuarios y contraseñas.
- Seguridad en el sitio de trabajo.
- Ingeniería social.
- Seguridad en la web y el correo electrónico.
- Protección en línea.
- A dónde acudir por ayuda.

4.2. Medios de comunicación para ejecutar la estrategia

4.2.1. Inducción corporativa: Se trata de la capacitación de ingreso de los empleados de la **INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO,** en la cual se abordan temas de seguridad de la información y ciberseguridad con el objetivo de dar a conocer las políticas de seguridad de la institución y los riesgos a los que se está expuesto.

4.2.2. Boletines de correos electrónicos: Son mensajes de correo electrónico cuyo contenido gráfico y de texto es construido con el apoyo del área de seguridad de la información y ciberseguridad.

4.2.3. Fondo de escritorio: Son fondos de escritorio corporativos que contengan imágenes y mensajes cortos relacionados con la protección de la información de la institución, los cuales con diseñados en conjunto con el equipo de seguridad de la información y ciberseguridad.

4.2.4. Mensaje de carteleras y TV: Son mensajes para las carteleras ubicadas dentro de las instalaciones de la institución, sean físicas o digitales; los temas a abordar partirían de los propuestos en el listado inicial y serán diseñados en conjunto con el equipo de seguridad de la información y ciberseguridad.

4.2.5. Concursos: Pruebas para motivar la participación de funcionarios y contratistas a las iniciativas de toma de conciencia. Por ejemplo, utilizar fondos de pantalla de oficinas inseguras para que los participantes busquen las situaciones indeseadas que se presentan en esta ilustración. La definición del premio depende de los recursos asignados por la **INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO**.

4.2.6. Conferencias: Presentaciones a las distintas áreas de la entidad, particularmente aquellas que representen un mayor nivel de riesgo frente a la protección de la información.

4.2.7. Contenidos en la intranet: Artículos, videos o ilustraciones relacionados con los temas indicados en el ítem 4.1. de este mismo documento.

4.2.8. Clases inducción estudiantes: Se propone integrar algunas clases de inducción a todos los estudiantes sobre las políticas institucionales de seguridad de la información y ciberseguridad y los riesgos existentes.

4.2.9. Servicios contratados externamente: dependiendo de la disponibilidad presupuestal será posible el fortalecimiento de la estrategia de toma de conciencia a través de proveedores externos especializados que permitan nuevas alternativas de comunicación como:

- Juegos o contenido interactivo.
- Interpretaciones u obras de teatro.
- Conferencias especializadas.
- Cursos.

4.3. Factores de Éxito

La eficaz ejecución de la estrategia propuesta depende del cumplimiento de los siguientes atributos:

- Inclusión de todas las partes interesadas.
- Aprovechamiento de los medios de comunicación internos.
- Apoyo de todas las áreas en las iniciativas de concientización.
- Segmentación de público objetivo en conjunto con el área de comunicaciones.
- Énfasis en casos (reales o hipotéticos), en vez de contenidos técnicos.
- Apoyo de la alta dirección.
- Búsqueda de diferentes alternativas en la forma en la cual se pretende hacer llegar el mensaje a sus destinatarios.

4.4. Desarrollo de la Estrategia: Temas Vs Medios de Comunicación

Temas \ Medios de Comunicación	Inducción Institucional	Boletines	Fondos de Escritorio	Carteleras	Concurso	Conferencias	Servicios Externos	Intranet	Clases Inducción
Políticas de seguridad de la compañía.	X		X	X	X	X	X	X	X
Procesos y procedimientos del MSPI.						X	X	X	
Manejo de usuarios y contraseñas.	X	X		X	X		X		X
Seguridad en el sitio de trabajo.	X			X	X		X		
Ingeniería social.		X	X	X			X		X
Seguridad en la web y el correo electrónico.		X		X	X	X	X		
Protección en línea.		X			X	X	X		X
A dónde acudir por ayuda.	X		X		X			X	X

4.5. Desarrollo de la Estrategia: Temas Vs Calendario

Calendario / Temas	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Políticas de seguridad de la compañía.												
Procesos y procedimientos del MSPI.												
Manejo de usuarios y contraseñas.												
Seguridad en el sitio de trabajo.												
Ingeniería social.												
Seguridad en la web y el correo electrónico.												
Protección en línea.												
A dónde acudir por ayuda.												

5. INDICADORES

- Número de eventos llevados a cabo vs porcentaje de cobertura de éstos.
- Temas abordados y/o desistidos.
- Resultados de evaluaciones periódicas en pruebas de seguridad orientadas a la ingeniería social y vulnerabilidad humana, lo que permitirá conocer el nivel de penetración del mensaje y le generación de cultura de seguridad.

6. REGISTROS

- Piezas de comunicación.
- Artículos.
- Registros de asistencia y demás soportes de las iniciativas realizadas.

Estos registros servirán como evidencia y podrán ser exigidos por lo entes de control y en las diferentes auditorías internas y externas que se realicen al MSPI en la institución.