**Plan de Campaña de mejores prácticas en Ciberseguridad**

En la era digital actual, la ciberseguridad se ha convertido en un elemento muy relevante para proteger los activos de las empresas y la información de sus clientes. Para fortalecer la postura de seguridad de las organizaciones, el Magíster en Tecnologías de la Información (MTI) de la Universidad Técnica Federico Santa María en conjunto con Business Continuity SpA ha desarrollado una propuesta complementaria de Plan de Campaña de Concientización en Ciberseguridad con las mejores prácticas a seguir implementadas en diversas actividades que se agrupan en el presente Plan.

Reconociendo la importancia de una difusión efectiva, se ha elaborado una propuesta de plan de difusión integral estratégico. Este plan tiene como objetivo asegurar que la información sobre ciberseguridad llegue a cada usuario final de manera efectiva, permitiendo que todos comprendan y apliquen estas prácticas en su trabajo diario.

**(ALGUNAS) Recomendaciones alternativas de difusión:**

* Enviar comunicado inicial de inicio de la campaña y de los objetivos a lograr en Ciberseguridad como Cambio Cultural.
* Distribuir/Disponibilizar las cápsulas-video por distintos medios de comunicación internos, con frecuencia semanal.
* Enviar un correo electrónico y publicación en la intranet de anuncio del Gerente General sobre la importancia de la ciberseguridad para los objetivos estratégicos de la empresa.
* Enviar un correo electrónico y publicación en la intranet de anuncio (equivalente al del Gerente General) pero emitido por algún usuario “referente” y reconocido de la empresa sobre la importancia de la ciberseguridad en las tareas cotidianas de su quehacer.
* Crear una sección dedicada en la intranet de la empresa para Disponibilizar las infografías con cierta frecuencia establecida.
* Compartir infografías derivadas de los slides en los canales de comunicación interna con cierta frecuencia establecida.
* Organizar sesiones de preguntas y respuestas con el equipo de RIESGOS sobre el contenido.
* Incorporar los puntos clave de los slides en las reuniones departamentales regulares, como Key Points semanales.
* Desarrollar una campaña de recordatorios visuales (protectores de pantalla, banners) con información de los slides.
* Crear un concurso de conocimientos basado en el contenido de las infografías.
* Establecer un programa de "embajadores de ciberseguridad" para promover y explicar el contenido entre compañeros.
* La ciberseguridad afecta a todos: planificar capacitaciones focalizadas según la temática a los distintos grupos de interesados en la organización.
* Efectuar “Laboratorios” que puedan mostrar prácticamente qué sucede cuando ocurren brechas en la ciberseguridad

**Propuesta de planificación de 10 potenciales iniciativas… (Crea las tuyas)**

1. **Enviar un correo electrónico de anuncio del Gerente General y luego otras colaboraciones sobre la importancia de la ciberseguridad**

* **Objetivo:** Captar la atención de todos los empleados desde los niveles más altos de la empresa.
* **Acción:** El Gerente General enviará un correo electrónico enfatizando la importancia de la ciberseguridad y cómo afecta tanto a la empresa como a los individuos. Incluirá una visión general de la campaña de sensibilización y las acciones que se tomarán a lo largo del mes y su continuidad posterior. Luego, lo mismo; pero con otros usuarios del entorno operacional, señalando su punto de vista desde su ámbito operacional.
* **Consejo práctico:** El correo debe tener un tono inspirador y realista, subrayando la responsabilidad compartida. Se puede incluir un video breve donde el Gerente General refuerce el mensaje visualmente. IDEM con otros “personajes” referenciables del entorno operacional (Ej. Operarios, Personal de aseo, Secretarias, Ingenieros de planta,..)

1. **Crear una sección dedicada en la intranet de la empresa para alojar los slides y videos**

* **Objetivo:** Proporcionar un espacio centralizado y accesible para que los empleados puedan consultar el contenido.
* **Acción:** Configurar una sección especial en la intranet donde se aloje todo el material de la campaña, como los slides de las presentaciones y cualquier recurso adicional.
* **Consejo práctico:** Asegúrate de que sea fácil de encontrar y navegar. Coloca un banner destacado en la página principal de la intranet para atraer la atención de los empleados.

1. **Compartir infografías derivadas de los slides en los canales de comunicación interna**

* **Objetivo:** Simplificar la información clave para hacerla más fácil de digerir y recordar.
* **Acción:** Usar o adaptar infografías visualmente atractivas basadas en los puntos clave de los slides y distribuirlas en los canales de comunicación interna, como el correo electrónico, Microsoft Teams o Slack. No olvidar la versión IMPRESA para difundir en paneles o murales de las distintas secciones de la empresa.
* **Consejo práctico:** Las infografías deben ser concisas y contener datos prácticos o estadísticas alarmantes que resalten la necesidad de aplicar buenas prácticas de ciberseguridad. Usa temas recurrentes como "Protege tus contraseñas" o "Ten cuidado con los correos electrónicos sospechosos". USA LAS INFOGRAFÍAS proporcionadas, cambiando ACME por el LOGO de tu empresa y luego distribúyelas por todos los medios posibles, tus RRSS, que no te limite lo que nunca antes se ha hecho.

1. **Organizar sesiones de preguntas y respuestas con el equipo de RIESGO sobre el contenido**

* **Objetivo:** Fomentar la interacción directa entre los empleados y el equipo de RIESGO para aclarar dudas.
* **Acción:** Programar sesiones de preguntas y respuestas con el equipo de RIESGO para que los empleados puedan hacer preguntas sobre el contenido de los slides o videos y cómo pueden aplicar las recomendaciones en su día a día.
* **Consejo práctico:** Estas sesiones pueden organizarse a través de videoconferencias o de forma presencial, y se recomienda que sean grabadas y almacenadas en la intranet para futuras consultas.

1. **Incorporar los puntos clave de los slides en las reuniones departamentales regulares**

* **Objetivo:** Asegurar que la ciberseguridad esté en la mente de los empleados a lo largo del tiempo, no sólo durante el MES de …
* **Acción:** Durante las reuniones departamentales regulares, los jefes de área deben presentar los puntos clave de los slides y discutir cómo se aplican al trabajo específico del equipo.
* **Consejo práctico:** Proporciona a los líderes de equipo una guía con ejemplos concretos que puedan personalizar para su equipo. También se pueden incluir estudios de caso breves sobre incidentes recientes de ciberseguridad.

1. **Desarrollar una campaña de recordatorios visuales (protectores de pantalla, banners) con información de los slides**

* **Objetivo:** Mantener la concienciación constante con elementos visuales en el entorno de trabajo.
* **Acción:** Crear protectores de pantalla, banners y otros elementos visuales que se coloquen en áreas comunes (digitales o físicas) para reforzar los mensajes clave sobre ciberseguridad.
* **Consejo práctico:** Usa gráficos llamativos y mensajes simples pero efectivos. Puedes actualizar los protectores de pantalla y banners cada semana con diferentes temas, como contraseñas seguras, correos phishing, uso de dispositivos personales (BYOD), etc.

1. **Crear un concurso de conocimientos basado en el contenido de los slides y videos.**

* **Objetivo:** Aumentar la participación de los empleados de manera lúdica y reforzar el aprendizaje.
* **Acción:** Organizar un concurso de conocimientos en el que los empleados respondan preguntas basadas en el contenido de los slides (infografías) y videos. Las respuestas correctas podrían otorgar puntos, y los ganadores recibirían premios (como días libres adicionales, tarjetas de regalo, gadgets, etc.).
* **Consejo práctico:** ¡Utiliza plataformas interactivas como Kahoot! o formularios en línea para organizar el concurso de forma atractiva y accesible para todos.

1. **Establecer un programa de "embajadores de ciberseguridad" para promover y explicar el contenido entre compañeros de labores.**

* **Objetivo:** Crear una red de apoyo dentro de la empresa, tipo monitores o embajadores, que mantenga vivo los mensajes usados en la campaña.
* **Acción:** Identificar y capacitar a un grupo de empleados en cada departamento para que actúen como "embajadores de ciberseguridad". Estos embajadores serán responsables de recordar y promover buenas prácticas entre sus compañeros, así como de responder preguntas básicas.
* **Consejo práctico:** Ofrece incentivos para los embajadores, como certificados o reconocimiento formal por parte de la dirección. También podrían recibir capacitación adicional por parte del equipo de TI para ampliar sus conocimientos.

1. **Planificar capacitaciones focalizadas según la temática a los distintos grupos de interesados en la organización.**

* **Objetivo:** No todos los conceptos de Ciberseguridad son aplicables a todos los miembros de la organización: es necesario focalizar y capacitar sobre nuevos procesos y conocimientos
* **Acción:** clasificar los conceptos de Ciberseguridad según los roles y puestos de los miembros de la organización. Existen roles más críticos que otros, así como existen conceptos que aplican a unos u otros grupos de trabajo, por lo que los conocimientos deben ser segmentados.
* **Consejo práctico:** Relevar el conocimiento previo de un equipo de trabajo sobre los conceptos que se quieran introducir o reforzar. Eso ayudará a focalizar aún más el proceso de capacitación, como a conocer los riesgos operativos existentes.

1. **Efectuar “Laboratorios” que puedan mostrar prácticamente qué sucede cuando ocurren brechas en la ciberseguridad**

* **Objetivo:** Poder demostrar, en la práctica, los efectos y resultados de “bajar la guardia” en ciberseguridad.
* **Acción:** Planificar y efectuar laboratorios (con una audiencia) en donde se pueda verificar, in situ, los resultados de brechas de ciberseguridad utilizando al equipo de Ethical Hacking que simulen ataques y se puedan demostrar los efectos de un ataque (en función del riesgo al que los roles objetivos estén expuestos).
* **Consejo práctico:** La capacitación es más efectiva cuando se puede demostrar lo que sucede cuando se baja la guardia. Efectuando ataques simulados en vivo, el público objetivo va a poder entender el impacto de no ejecutar las buenas prácticas de ciberseguridad.