Concientización, Deseo y Entrenamiento de Ciberseguridad

Política Global

OBJETIVO

Establecer el programa de concientización y entrenamiento de seguridad que permita difundir una cultura de Ciberseguridad involucrando a todos los colaboradores de Sigma.

DEFINICIONES

Ciberseguridad:
Conjunto de procedimientos y herramientas que se implementan para proteger la información y los procesos operativos y/o administrativos que se generan y ejecutan a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

Ingeniería Social:
Conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con programas malignos o abran enlaces a sitios infectados.

Phishing, Vishing y Smishing:
Se refiere al envío de correos electrónicos (Phishing), llamadas telefónicas (Vishing) o mensajes de texto (Smishing) haciéndose pasar por fuentes de confianza – como bancos, compañías, entre otros – pero que en realidad pretenden manipular al receptor para robar información confidencial / credenciales.

Los responsables de Seguridad de la Información de cada Unidad de Negocio deberán definir, planear, crear y ejecutar el programa de concientización y entrenamiento de Ciberseguridad en Sigma.

Los colaboradores con personal a su cargo deberán garantizar que su equipo participe en las actividades de concientización y entrenamiento de Ciberseguridad cuando sea requerido.

Todo colaborador deberá completar las actividades de entrenamiento en materia de Ciberseguridad, de asistir a las reuniones correspondientes y cumplir con las Políticas, leyes y reglamentos aplicables en todo momento.

Requerimientos:

El objetivo del programa de concientización y entrenamiento de Ciberseguridad es garantizar que todos los colaboradores alcancen y mantengan al menos un nivel básico de comprensión de los asuntos relacionados con la Ciberseguridad, incluyendo las obligaciones generales en virtud de las diversas Políticas, Procedimientos, normas, directrices, leyes, reglamentos, condiciones contractuales, normas éticas y de comportamiento aceptables.

Los responsables de Seguridad de la Información de cada Unidad de Negocio deberán identificar las áreas y personal crítico que suelen ser objetivo de ataques cibernéticos, con el fin de aplicar planes de entrenamiento específicos y avanzados. Los colaboradores que desempeñen funciones en materia de Ciberseguridad deberán contar con planes de entrenamiento avanzados de Ciberseguridad acorde a sus funciones.

Estos requisitos de entrenamiento deberán identificarse en los planes de formación departamental y financiarse en consecuencia. Los requisitos de entrenamiento deberán reflejar la experiencia previa, la educación y/o las cualificaciones profesionales, así como los requisitos de trabajo previstos.

Las actividades de concientización y entrenamiento en materia de Ciberseguridad deberán comenzar desde el proceso de ingreso a la organización. Los colaboradores deberán llevar a cabo un curso de inducción a la Ciberseguridad de forma presencial o en línea indicado por los responsables de Seguridad de la Información de cada Unidad de Negocio.

Siempre que sea necesario y factible, los materiales y ejercicios de concientización y entrenamiento deberán adaptarse a los destinatarios en términos de idioma, cultura, estilos, formatos, complejidad, contenido técnico, entre otros.

Los responsables de Seguridad de la Información de cada Unidad de Negocio deberán proporcionar a los colaboradores de Sigma la ubicación de los materiales de concientización y entrenamiento de Ciberseguridad, junto con las Políticas de seguridad, las normas y la orientación de asuntos relacionados con la Ciberseguridad.

Concientización de Ciberseguridad:

Los responsables de Seguridad de la Información de cada Unidad de Negocio deberán crear y fortalecer la conciencia de Ciberseguridad en Sigma a través de actividades como:

- El envío de correos electrónicos con noticias relevantes, avisos, guías y recomendaciones de Ciberseguridad.
- La programación de seminarios en línea o presenciales para fortalecer tópicos específicos en materia de Ciberseguridad.
- La creación de contenido audiovisual como videos o imágenes de Ciberseguridad.

Entrenamiento de Ciberseguridad:

Todo colaborador de Sigma, al momento de su contratación y posteriormente de forma anual, deberá completar de forma satisfactoria el entrenamiento de Ciberseguridad asignada. Algunas áreas y colaboradores podrán ser requeridos a completar módulos de entrenamientos adicionales en función de los requisitos específicos de su puesto.

Los colaboradores dispondrán de 15 días hábiles para completar cada curso. En caso de encontrarse en un periodo vacacional o similar no se contarán estos días.

Los responsables de Seguridad de la Información de cada Unidad de Negocio deberán notificar a los colaboradores del entrenamiento asignado y enviar recordatorios de forma continua. En caso de no cursar el entrenamiento asignado en las tres semanas definidas, los responsables de Seguridad de la Información de cada Unidad de Negocio, en conjunto con los responsables de Capital Humano, deberán definir la sanción correspondiente.

Ataques Simulados de Ingeniería Social:

De forma periódica, el área de Seguridad de la Información deberá llevar a cabo ejercicios de Ingeniería Social simulada, incluyendo Phishing, Vishing, Smishing, pruebas de USB, evaluaciones físicas, entre otros. Estas pruebas se aplicarán bajo un calendario anual establecido, conocido únicamente por los responsables de Seguridad de la Información de cada Unidad de Negocio. Algunos de estos ataques se dirigirán contra departamentos o individuos específicos en función de la determinación del riesgo.

En caso de que un colaborador sea víctima de un ataque simulado, el responsable de Seguridad de la Información de la Unidad de Negocio correspondiente deberá notificarle inmediatamente, especificando las acciones a seguir. El propósito de dichas acciones es reforzar el nivel de conciencia de los colaboradores, con el fin de proteger la información y activos de Sigma.

En caso de incumplimiento a la presente Política, pese a las acciones de reforzamiento, se aplicarán medidas correctivas definidas por cada Unidad de Negocio, incluyendo más no limitándose a sesiones de retroalimentación en conjunto con su jefe inmediato, bloqueo temporal de cuentas de red, entre otras sanciones.

Los responsables de Seguridad de la Información de cada Unidad de Negocio deberán fomentar el reconocimiento a los colaboradores de Sigma que superen las expectativas del programa de Ciberseguridad.