Es responsabilidad de grupo GIM y sus filiales asegurar que la información y datos estén a salvo de usuarios malintencionados, creando y ejecutando un Plan integral de concientización sobre seguridad cibernética que eduque a los usuarios sobre las principales ciber amenazas.

El plan denominado "Plan Integral de Ciberseguridad GIM" tiene como objetivo concientizar a los usuarios sobre el uso correcto y seguro de los recursos informáticos que utiliza en la red de datos GIM y medio ambiente a su alcance, para disminuir la probabilidad de vulnerabilidades que puedan ser explotadas por individuos maliciosos.

Este Plan anual consistirá en informar a los usuarios de la red de datos GIM mediante los medios de: **correo electrónico institucional, Intranet y estados de WhatsApp**, sobre como:

- Reconocer posibles ciberataques.
- Las señales de ingeniería social.
- Los peligros del malware y utilización de software gratuito.
- Cómo proteger los datos confidenciales de una violación de datos.
- Ataques de phishing.

Este Plan debe de ofrecer información actualizada y en constante evolución para mantener la seguridad de los datos ante la constante amenaza de las sofisticadas técnicas utilizadas por los ciberdelincuentes y disminuir la probabilidad al mínimo de que un usuario ingrese a un link malicioso, mediante los siguientes procesos y acciones.

1.- Se identifica a los usuarios de la red de datos GIM como la parte más débil en cuanto a seguridad de la información se refiere, ya que son objetivos constantes de personas maliciosas que mediante ataques específicos de ingeniería social a través de correos electrónicos, mensajes de WhatsApp y SMS, enfocados en engañar a los destinatarios para que hagan clic en enlaces o abran archivos adjuntos, por lo tanto, es responsabilidad del usuario de la red de datos GIM y filiales, el conocer los lineamientos actuales que rigen la utilización de recursos de Software y Hardware que les fueron asignados y los medios de comunicación utilizados para ingresar a la red de datos GIM.

2.- La empresa debe de proveer soluciones como antivirus, sistemas de detección de intrusos (EDR), sistemas de prevención de intrusiones perimetral, sistemas de prevención para correo electrónico, que son soluciones técnicas para la protección de la información en cada uno de los equipos utilizados dentro de la red de datos GIM.

3.- Concientizar a los usuarios sobre posibles ataques de ciberseguridad dirigidos a ellos a través de phishing, para que comprendan lo que se requiere de ellos y se comprometan a seguir los lineamientos establecidos en el grupo GIM y sus filiales sobre la utilización de recursos asignados y publicados en la intranet.

4.- Es responsabilidad del área de Tecnologías de Información dar a conocer a los usuarios de la red de datos GIM, a través de los medios mencionados previamente en este plan (**correo electrónico institucional, Intranet y estados de WhatsApp)** sobre ciberseguridad, distintas formas de ataques de phishing, a través de la creación y difusión de videos cortos y concisos sobre ciberseguridad, la creación de artículos y también breves mensajes de concientización sobre el tema.

5.- Es responsabilidad del área de Tecnologías de Información medir la efectividad del Plan mediante una encuesta inicial y trimestrales posteriores que evidencien el comportamiento del Plan y su evolución, así como el grado de concientización del usuario para lograr identificar a los que requieran formación adicional.

6.- La información proporcionada a los usuarios a través de los medios de comunicación mencionados previamente, deberá ser de calidad y tomada de fuentes de información de proveedores de seguridad informática, hardware y software fiables como, Crowdstrike, Fortinet, Microsoft, John Deere, Oracle Cloud, Know4, Lenovo, Alestra CSIRT, Arcserve UDP.

7.- Se deberá de enviar y publicar de forma masiva el spot de información sobre ciberseguridad elegida y dirigida a todos los usuarios de la red de datos GIM y filiales durante la primera semana de cada mes por personal de Tecnologías de Información.