Protección y prevención

1. Verificación de Identidad:

* Antes de compartir información confidencial o acceder a enlaces proporcionados por terceros, verifica la identidad de la persona o entidad con la que estás interactuando. Usa canales de comunicación confiables para confirmar la autenticidad.

1. Cautela en Comunicaciones:

* Sé cuidadoso con los correos electrónicos, mensajes y llamadas telefónicas inesperadas o que soliciten información personal o sensible. Si algo parece sospechoso, verifica la autenticidad antes de proporcionar datos.

1. Configuración de Privacidad en Redes Sociales:

* Ajusta la configuración de privacidad en tus perfiles de redes sociales para limitar la información que se comparte públicamente. Evita revelar detalles personales que puedan ser utilizados en ataques de ingeniería social.

1. Autenticación de Múltiples Factores (AMF):

* Utiliza la autenticación de múltiples factores siempre que sea posible. Esto añade una capa extra de seguridad al requerir no solo una contraseña, sino también un segundo método de verificación.

1. Actualización y Seguridad de Dispositivos:

* Mantén actualizado tu software y sistema operativo. Las actualizaciones a menudo incluyen parches de seguridad que pueden proteger contra vulnerabilidades utilizadas en ataques de ingeniería social.

1. Formación y Políticas Empresariales:

* En entornos corporativos, proporciona formación en seguridad a los empleados y establece políticas claras sobre el manejo de información confidencial y la validación de solicitudes.

1. Desarrollo de un Sentido Crítico:

* Fomenta un enfoque crítico al interactuar en línea. Cuestiona la legitimidad de solicitudes o mensajes sospechosos y no tomes decisiones apresuradas sin verificar la información.