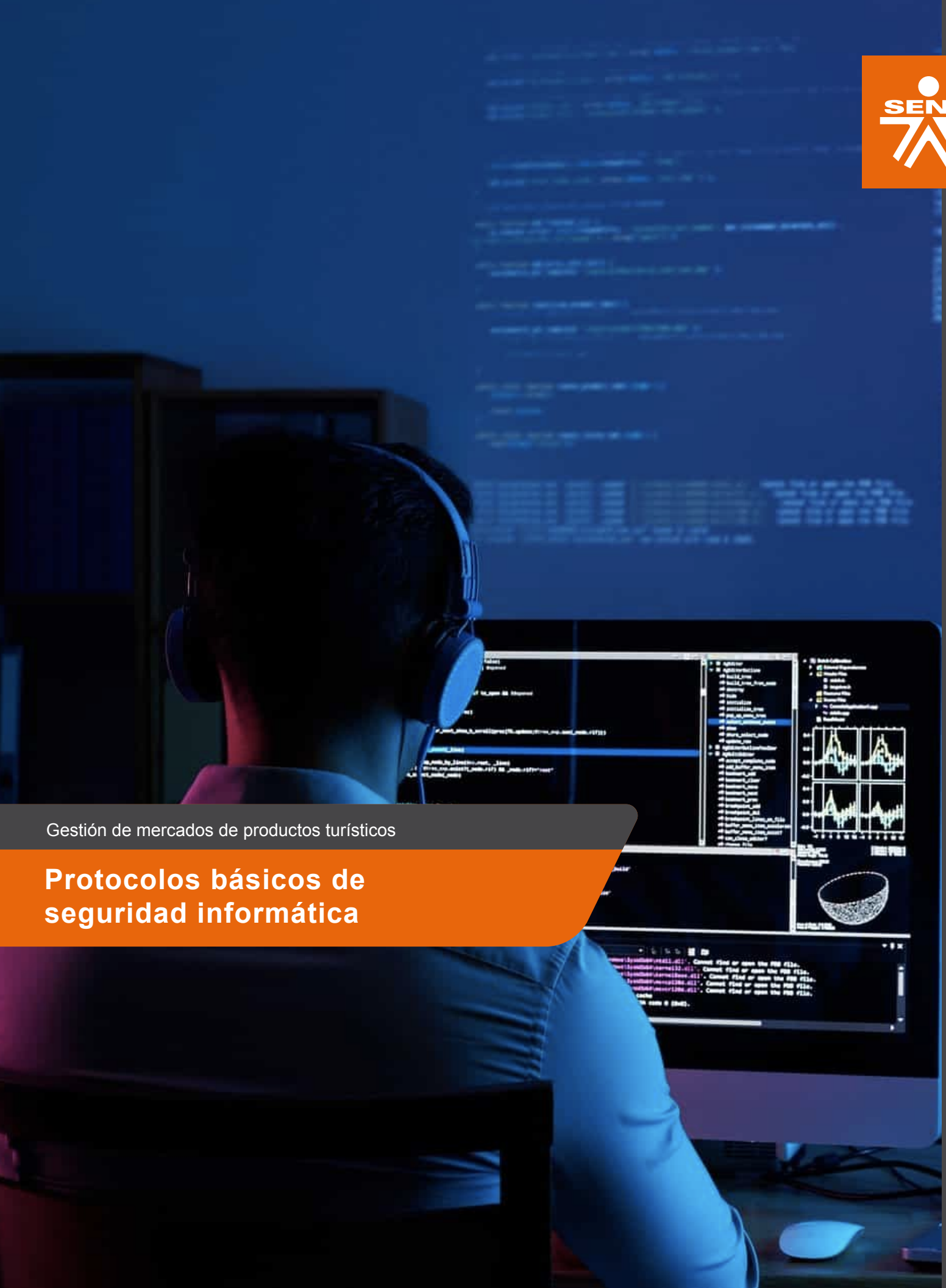

Gestión de mercados de productos turísticos

Protocolos básicos de seguridad informática

Servicio Nacional de Aprendizaje SENA

Protocolos básicos de seguridad informática

Para impedir infracciones de seguridad en la red, se debe instaurar un plan de *ciber* seguridad que sea conocido por todos los participantes. Así es como se agiliza el acceso seguro a los datos, evitando fugas y optimizando la credibilidad de los clientes. Las etiquetas de seguridad de la información deben tener en cuenta:

- **Prevención de pérdida de datos (DLP).** Se requiere imposibilitar que los individuos tengan acceso a datos críticos no pertinentes y que sean reenviados externamente. Por eso, para lograr prevenir lo anterior, se necesita de una capacitación oportuna para los empleados.
- **Requerimientos de claves.** Se deben instaurar medidas teniendo en cuenta la complejidad de las claves, dónde y cómo guardarlas, con qué frecuencia actualizarlas. Si esto se realiza de manera periódica, garantiza los lineamientos de seguridad de la información.
- **Administración de información confidencial.** Aclarar en qué momento los participantes pueden compartir datos sensibles con otras personas o empresas, cómo identificarlos y destruirlos cuando se requiera. De igual forma, se debe precisar en qué momento es adecuado compartir el correo electrónico corporativo, cómo bloquear, hacer reporte de *spam* (correo no deseado) y de sitios *web* dudosos.

Para fomentar la cultura colaborativa de la empresa y mantener resguardados sus datos confidenciales, es preciso tener actualizados a los participantes con relación a los lineamientos y normatividad de seguridad de la información. Se debe aclarar cuál es el marco normativo de la seguridad de la información para proteger la prolongación de un negocio y poder vigilar los peligros de cualquier evento. (Función Pública, 2020)