Conceptos relevantes de seguridad año 2022

1. Ciberseguridad: protección de los sistemas informáticos, redes y dispositivos de una organización contra ataques cibernéticos y amenazas.
2. Ciberdefensa: medidas y estrategias para proteger los sistemas informáticos y la infraestructura crítica de una organización o país contra ataques cibernéticos.
3. Seguridad en la nube: protección de los datos y sistemas alojados en la nube contra ataques y violaciones de seguridad.
4. Ciberinteligencia: recopilación y análisis de información sobre amenazas cibernéticas y actores maliciosos para tomar decisiones informadas en términos de seguridad.
5. Autenticación de múltiples factores (MFA): medida de seguridad que requiere que el usuario proporcione varios medios de autenticación, como una contraseña y un código de un dispositivo móvil, antes de acceder a un sistema o recurso.
6. Cibercrime: delitos cometidos a través de medios informáticos, como el robo de datos, el fraude y el espionaje cibernético.
7. Ransomware: tipo de malware que cifra los archivos de un usuario y exige un rescate para proporcionar la clave de descifrado.