Término	Definición
ACLs	Siglas de "*Access Control Lis*t". Es un conjunto de reglas que se utilizan para controlar el acceso a recursos de red, como archivos, carpetas, dispositivos o servicios.
Activos tecnológicos	Infraestructura de cómputo o software que utiliza la empresa para apoyar sus operaciones, como computadoras, servidores, dispositivos móviles, bases de datos, etc.
BCP	Siglas de "*Business Continuity Planning*". Es un proceso de gestión de riesgos que permite a una organización mantener sus operaciones críticas y minimizar el impacto de interrupciones no planificadas en su funcionamiento.
BYOD	Siglas de "*Bring Your Own Device*". Se refiere a permitir a los empleados usar sus propios dispositivos personales, como teléfonos inteligentes, tablets y computadoras portátiles, para realizar sus funciones laborales.
Centros de datos	Es una instalación física que se utiliza para alojar y administrar sistemas informáticos y de telecomunicaciones utilizados para almacenar, procesar y distribuir datos.
Cifrado	Es un proceso mediante el cual se codifica información legible de tal manera que solo puede ser entendido por aquellos que poseen los medios para descifrado, de tal forma que no sea leída por personal no autorizado.
Conexión remota	Es la capacidad de acceder y controlar un dispositivo o sistema informático desde una ubicación distinta a la del mismo dispositivo o sistema a través de Internet.
Continuidad del negocio	Es la capacidad de una organización para mantener sus operaciones críticas y minimizar el impacto de interrupciones no planificadas, como desastres naturales, interrupciones del suministro eléctrico, fallas en la tecnología o ataques cibernéticos.
CSC	Siglas de "*Cloud Service Customer*". Es la organización o persona que utiliza un servicio en la nube para alojar, procesar o almacenar sus datos.
CSP	Siglas de "*Cloud Service Provider*". Es la empresa o un proveedor que ofrece servicios en la nube a través de un modelo de negocio basado en la suscripción.
DDoS	Siglas de "*Distributed Denial of Service*". Es un tipo de ataque informático desde múltiples fuentes distribuidas lógica o geográficamente que busca llevar al limite de capacidad los recursos con el fin de interrumpir un servicio publicados en Internet.
DRP	Siglas de "*Disaster Recovery Planning*". Es un proceso de gestión de riesgos que permite a una organización recuperar sus servicios tecnológicos ante interrupciones graves y no planificadas en sus operaciones críticas.
EDR	Siglas de "*Endpoint Detection and Response*". Es una solución de seguridad informática que se utiliza para detectar, investigar y responder a amenazas en dispositivos finales, como computadoras de escritorio, laptops, servidores y dispositivos móviles.
Enlaces dedicados	Es un tipo de conexión de red que se establece entre dos puntos específicos para proporcionar una conexión con ancho de banda exclusivo.
FTPS	Siglas de "*File Transfer Protocol Secure*". Es una versión segura del protocolo de transferencia de archivos "File Transfer Protocol".
Infraestructura de TI	Es el conjunto de componentes físicos, software, redes y servicios necesarios para operar y administrar sistemas de información.
ISO-27001	Es una norma estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información.
líneas base de seguridad	Es un conjunto de opciones de configuración que buscan asegurar que los equipos cuenten con los servicios esenciales de manera consistente con un nivel mínimo de seguridad.
Niveles de Servicio	Es un acuerdo contractual entre un proveedor de servicios y un cliente, que define los objetivos de desempeño para un servicio y la forma de medición con base a los términos y condiciones del servicio ofrecido, incluyendo de manera enunciativa mas no limitativa las disponibilidad esperada del servicio, los tiempos de respuesta en caso de un incidente o evento, los tipos de soporte prestados y las garantías en caso de falla o incumplimiento.

PCI-DSS	Siglas de "*Payment Card Industry Data Security Standard*". Es un conjunto de estándares de seguridad diseñados para proteger la información de tarjetas de pago, incluyendo tarjetas de crédito, débito y prepagos.
pententest (Prueba de Penetración)	Es una técnica de seguridad informática que simula un ataque controlado, con el objetivo de probar las defensas de seguridad que permitan identificar vulnerabilidades en la seguridad de sistemas, aplicaciones o redes informáticas.
Servidor NTP	Siglas de "*Network Time Protocol*". Es un protocolo de comunicación utilizado para sincronizar la hora de los dispositivos en una red informática
SLA	Siglas de "*Service Level Agreement*". Revise la definición de Nivel de servicio.
SOA	Siglas de "*Statement of Applicability*". Es un documento utilizado en el contexto de sistemas de gestión de seguridad de la información, donde se determinan los controles que son aplicables a la organización.
SOC 2	Es un informe éstandar de la industria emitido por revisores externos que evalúan los sistemas de información en términos de seguridad, disponibilidad, integridad y confidencialidad.
SOC 3	Es un informe éstandar de la industria emitido por revisores externos que evalúan los sistemas de información en términos de seguridad, disponibilidad, integridad y confidencialidad que considera su divulgación pública, proporcionando una visión general de alto nivel, sin revelar detalles específicos sobre los controles implementados.
SSAE	Siglas de "*Statement on Standards for Attestation Engagements*". Es un conjunto de estándares de auditoría desarrollado por la American Institute of Certified Public Accountants.
Tokenización	Es una técnica de seguridad que implica la sustitución del valor de un dato confidencial con un valor único no identificable y no relacionado con el dato original.
UEBA	Siglas de "*User and Entity Behavior Analytics*". Es una solución de seguridad informática que se utiliza para detectar y responder a amenazas internas y externas mediante el análisis del comportamiento de los usuarios y entidades dentro de una red.