GLOSARIO DE TERMINOS

Activo (Asset): Un recurso, procedimiento, sistema u otra cosa que tenga un valor para una organización y por lo tanto deba de ser protegida, los Activos pueden ser bienes físicos tales como equipos de cómputo y maquinaria, también puede ser la Información y propiedad intelectual.

Adware: Software legitimo pero molesto, es una característica que tienen algunos programas gratuitos o en fase de prueba que muestran publicidad, mensajes de activación o de compra, comúnmente el creador cobra por la publicidad que se muestra, los mensajes se muestran cuando esta en funcionamiento el software asociado.
Antivirus: Software diseñado para la detección, prevención y eliminación de Software mal intencionado o dañino para los sistemas.

Ataques de Diccionario: Es un tipo de ataque de fuerza bruta enfocado en el que se utiliza una lista predefinida de palabras.

Ataque de Fuerza Bruta: Es un tipo de ataque que consiste en que el atacante intenta con todas las posibles combinaciones de letras, números y caracteres para acertar la contraseña, PIN o phassphrace.

Auditoría: La verificación independiente de cualquier actividad o proceso.

Autenticación: El procedimiento de verificar la identidad que reclama un sujeto mediante una validación en un sistema de control de acceso**.**

Autorización: Es el proceso de definir los derechos o permisos asignados a un sujeto (que puede hacer).

Baja de Voltaje (Brownout): Voltaje bajo de manera prolongada de una fuente de energía eléctrica, tal como la energía eléctrica del servicio público.

Biometría: Cualquiera de varios métodos utilizados como parte de un mecanismo de autenticación, para verificar la identidad de una persona. Los tipos de biometría utilizada incluye las huellas dactilares, impresiones de la palma de la mano, firmas, escaneos de retina, escaneos de voz y patrones de escritura en teclados.

Certificado Digital: Es un certificado que liga una identidad a una llave de cifrado pública.

Cifrado: El proceso de transformar texto plano a texto cifrado**.**

Cifrar: Una transformación criptográfica de texto claro a mensaje cifrado.

Confidencialidad: Previene del uso no autorizado o revelación de información, asegurándose que la información es accesible únicamente para aquellos que tengan autorizado su uso**.**

Controles Detectivos: Controles que identifican violaciones e incidentes.

Controles Disuasivos: Controles que desalientas la realización de violaciones.

Criptoanálisis: Es la ciencia de descifrar texto cifrado sin el uso de la llave criptográfica.

Criptografía: La ciencia de cifrar o descifrar información, tal como puede ser un mensaje privado para proteger su confidencialidad, integridad y / o autenticidad.

Criptología: La ciencia que abarca Criptografía y Criptoanálisis.

DDoS (Ataque distribuido de negación de Servicios): Es un tipo de ataque en el que el atacante inicia ataques de negación de servicio simultáneamente desde muchos sistemas.

Defensa en profundidad (o en capas): Es el principio de proteger los activos (información, bienes físicos de la empresa, etc) por medio de utilizar varias capas de protección diferentes.

Descifrado: Es el proceso de transformar texto cifrado en texto plano.

Directrices (Guidelines): Documentos similares a Estándares, pero considerados recomendaciones, en lugar de un requisito forzosos.

Disponibilidad: El proceso de asegurar que los sistemas e información sean accesibles para usuarios autorizados cuando ellos lo requieran.

Due Care (Cuidado Necesario): Los pasos que toma una organización para implementar mejores prácticas de seguridad.

Due Diligence (Diligencia Debida): La prudente administración y ejecución de "Due Care".

Dumpster Diving (Buceo de Contenedores): El proceso de examinar basura con la intención de encontrar bienes valiosos o información.

Espionaje: La práctica de espiar o utilizar espías para obtener información propietaria o confidencial.

Firewall: Dispositivo o programa que controla el flujo de tráfico entre redes.

Firewall de Aplicaciones: Un Firewall que inspecciona la capa 7 del Modelo OSI (aplicación) con el objetivo de bloquear contenido malicioso antes de que alcancé o abandone el Servidor de Aplicaciones (portal web, base de datos, etc).

Forense (Informática Forense): La ciencia de conducir una investigación criminal computacional para poder determinar que sucedió o quien es el responsable por lo ocurrido.

Función Hash: Una función matemática que crea una representación única de un grupo grande de datos. Las funciones Hash son frecuentemente utilizadas en algoritmos criptográficos y para producir resúmenes de mensajes (Checksums and message digest).
Gateway: Un sistema conectado a una red de computadoras, el cual ejecuta cualquier traducción en tiempo real o funcionalidad de interfaz.

Honeypot: Un sistema señuelo instalado por un administrador de seguridad para descubrir los métodos de ataque de hackers potenciales.

Hot Site: Una ubicación alterna a la de uso diario, con recursos computacionales totalmente funcionales que tiene servicios de electricidad, aire acondicionado, servidores de impresión, servidores de archivos y estaciones de trabajo, en resumen todos los servicios brindados en la ubicación primaria.

Identificación: Los medios por los cuales un usuario reclama una identidad especifica sin validación a un sistema.

Integridad: Garantiza la exactitud y completitud de la información y los métodos de procesamiento.

Negación de Servicios (DoS): Es un ataque a sistemas o redes con la intención de hacer que el sistema o red no este disponible para su uso.

Propiedad Intelectual: Incluye patentes, marcas registradas, derechos de autor y secretos comerciales.

Pruebas de Caja Negra:Es un tipo de prueba de seguridad donde el sujeto que realiza la prueba no tiene ningún conocimiento previo de los sistemas que están siendo puestos a prueba.

Texto Cifrado (Ciphertext): Es un texto plano que ha sido transformado (cifrado) en un mensaje mezclado que es ininteligible.