

Ciberseguridad

Contents

Ciberseguridad	1
Libros	2
Prevenir	2
Fallo de Ciberseguridad	2
Terceros	2
Nube	3
Seguridad	3
Ciclo de demming	3
Seguridad	3
Seguridad de la Información	3
Ciberseguridad	3
Principios CIA y DAD	3
Control de seguridad	3
Tendencias de Gartner	4
Certificaciones	4
Entidades certificadoras	4
Ejercicio: nombrar 5 certificaciones de interés	5
Estándares ISO/SEC de ISMS. Familia 27000	5
Más categorías del 27000:2018	5
NIST, y demás estándares referencia	5
El error no solo es de computadoras	6
Como realizar un ataque	6
Protegerse	6
Formas verbales en los estándares	7
Estructura del ISO/IEC 27000:2018	7
Detección de vulnerabilidades	7
Comandos & Términos	7
Aplicaciones	8
ISMS	8
Politica	9
.....	9
Control de acceso	10
Politica de control de acceso	10
IAM	10
Tendencias Gartner	10
Etapas	10
Arquitectura de seguridad	11
Criptografia	11
Criptografia	11
Hash	11
Kerberos	11
X.509	11
Herramientas	12

Entrega de proyecto 4 diciembre

Libros

The Tao of network monitoring

Prevenir

Ahora mismo estamos hablando de la calse pasada, de cómo vimos que se podía vulnerar cualquier dispositivo, donde con un panel de control se pueden realizar acciones desde el exterior.

- MDM: Mobile Device Management

Entre las medidas para prevenir los ataques tenemos:

- Hacer uso de antivirus
- Utilizar un MDM para notificación de
- No estar descargando software que no es de fiar
- Dar platicas de conscientización a los que nos rodean
- Monitorear la actividad de los dispositivos para detectar anomalías
- No se puede confiar 100% en las aplicaciones de tiendas oficiales
 - Por esto es necesario checar los permisos que solicitan las aplicaciones
 - En caso de que requiere muchos permisos podemos buscar aplicaciones que usen menos permisos
 - Si somos los desarrolladores debemos verificar que estamos poniendo los permisos esenciales y ya

Fallo de Ciberseguridad

En teconologia existe tanto los fallos de ciberseguridad y la desigualdad digital son varios de los riezos mas importantes que hay a nivel global, de la mano con el nivel de tecnología de los gobiernos.

Las fallas de seguridad que involucran las computadoras causan inestabilidad económica, perdidas económicas, intestabilidad social.

Los entes reguladores suelen aprender de los ataques, lo que implica que hasta que el daño esta hecho, creando las areas de seguridad después de perder. CISO: Chief Information Security Officer. Director de la ciberseguridad

Existe un gran deficit en las empresas y en los gobiernos en el tema de la ciberseguridad.

Terceros

No basta con contratar a terceros para gestionar servicios, pues la falta de estándares de seguridad y de confianza pueden resultar en que los mismos terceros de forma indirecta o directa posibiliten un flanco para ser vulnerados.

Muchas empresas se suelen inclinar del lado de los servicios de terceros debido al dinero y esfuerzo que requiere el mantener el hardware y software necesario para aumentar la seguridad.

Si se contratan terceros se debe de buscar auditar a los terceros, poniendo clausulas de contrato. El chiste es evitar a toda costa el filtrado de información.

Los fallos de ciberseguridad pueden crear cadenas de sucesos sociales negativos.

CIEM: Concentran todos los eventos. Si hay terceros entonces pueden observar todo lo que sucede.

Tambien existen riezos a nivel fisico, como cuando respaldas información en discos y por lo tanto el robo de información no se nota.

Nube

Cuando se utilizan servicios en la nube la responsabilidad sobre la seguridad es compartida.

Que el proveedor de servicios cumpla con sus certificaciones de seguridad no significa que la aplicación sea segura, como desarrolladores podemos vulnerar la seguridad de nuestro servicio como un todo al tener malas practicas a nivel de aplicación.

Seguridad

De *securitas*, que esta en un estado sin preocupaciones.

La seguridad es un proceso continuo, como decia el libro, en lugar de decir 'estamos seguros', la respuesta correcta es 'déjame revisar'.

Ciclo de demming

- Plan: Qué vamos a mitigar
- Do: Implementamos
- Check: Verificamos con retest o auditoria
- Act: Reacción

Seguridad

- Seguridad Informatica: Seguridad integral de los dispositivos
- Seguridad Información: Se encarga del ambiente digital y físico
- Ciberseguridad: Se encarga solo del ambiente digital

En estos puntos se busca:

- Integridad: La información se mantiene en un estado valido, confiable.
- Disponibilidad: Se encuentra disponible cuando se desea utilizar.
- Confidencialidad: Se encuentra solo expuesta a los entes autorizados.

<i>Se dice ente porque pueden ser personas, empresas, etc.</i>

Una cadena de custodia, al hacer una denuncia de un crimen en la cadena se registran los distintos dispositivos durante el proceso donde el perito extrae los indicios que se pueden convertir en evidencias. En esta custodia.

Seguridad de la Información

Se abarca la tecnologia, las personas y los procesos. Es decir, tanto lo

Ciberseguridad

Esta enfocada en el entorno digital, es el conjunto de herramientas, politicas, guias, análisis y acciones necesarios enfocados en lo digital.

Principios CIA y DAD

La confidencialidad, integridad y disponibilidad. Por sus siglas en ingles *Confidentiality, Integrity* y *Availability*.

Lo contrario a la CIA es la DAD, la alteración, destrucción o divulgación.

<i>La ISC2 es un ente de no se que. Menciona que es bueno rotar actividades</i>

Control de seguridad

Entre las distintas medidas que podemos tomar para proteger la información podemos tener politicas de:

- Integridad:
 - Permisos mínimos para los entes
 - Lo que implica controles de acceso.
 - Need to know: Que la persona solo sabe lo que *necesita* saber.
- Disponibilidad:
 - Tolerancia a fallas/redundancia
 - Ej. Dos fuentes de poder.
 - Clusters de alta habilidad (*HA Clusters*)
- Confidencialidad:
 - Segregación de privilegios
 - Rotación de actividades
 - Canales encubiertos
 - Análisis de tráfico
 - Cifrado
 - Controles de acceso

Tendencias de Gartner

Es una consultora que realiza estudios a nivel mundial que se toma como referencia para la seguridad.

- Se puede reducir en un 90% los impactos financieros si se adopta arquitectura segura.
- El 60% de empresas considerará la seguridad de terceros para realizar tratos.
- Preventivo no reactivo. Resiliencia, poder recuperarse de un efecto grave. No es un gasto, es solo medidas preventivas para prevenir más gastos/pérdidas.
- Hay proveedores y fabricantes específicos de seguridad que desarrollan hardware para bases de datos, etc.
- Se prevee que la ciberseguridad tome mucha fuerza, se creen comités de seguridad.
- Desde 2020 se habla de la ciber-resiliencia.
- Los que vulneran pueden tomar los artefactos vulnerados como arma.

Nota: Un solo proveedor trae desventajas como que todos tengan las mismas vulnerabilidades, así como que si el principal es atacado no tienes a donde moverte.

Certificaciones

Hay distintas certificaciones que van desde seguridad, inteligencia artificial, computo en la nube, seguridad. A nivel de persecución económica un project manager ya no es tan valioso.

Entre las certificaciones más solicitadas esta:

- CISP: Para cargos altos, es para nivel diseño, es muy completo, incluye de todo. Es como una maestría
 - Necesita 5 años de experiencia
 - Estudios solo cuentan como un año en algunos casos
- CISA: Auditoria de sistemas
- OSCP, OSCE: Ofensivo
- CEH: Certified hacker
- EJPJG: Pentester junior

Entidades certificadoras

- ISC2: Muy valorado, hay ahora mismo uno abierto
 - Certificado en Ciberseguridad: Básico, gratis (<https://isc2.org/certifications/cc>)

- EC-Council
 - Ethical Hacking Essentials
 - Y más (<https://www.eccouncil.org/cybersecurity-exchange/cyber-novice/free-cybersecurity-courses-beginners/>)
- ISACA
- Offensive Security
- Sans Institute

Los posgrados tienen más peso a largo plazo y en las oportunidades que se pueden tener pues aprendes a nivel profundo sobre los temas que se tratan.

En las certificaciones solo se evalúa herramientas y puntos específicos, está bien tenerlas pero mejor primero maestría.

No hay que quedarse en una sola herramienta.

Laboratorio: Hack-mex

Algunas de las herramientas de seguridad de software es CSSLP

Ejercicio: nombrar 5 certificaciones de interés

CSSLP,

Estándares ISO/SEC de ISMS. Familia 27000

Tenemos la familia de los 27000 que nos especifican

- terminología
- especificaciones
- buenas prácticas
- guías de implementación de medidas de seguridad
- medición, análisis, evaluación
- gestión de información privada
- etc

Seguridad de la información vs privacidad: De la información implica todas las formas, como física, los discos, lo que hablan las personas, etc sobre la información que debemos proteger. En cambio la privacidad lo que hace es que se protegen los datos que permiten identificar personas.

Las certificaciones son 27001, 27002, 27003, 27004, 27005, 27701:2019

Más categorías del 27000:2018

Tarea entrar en la página del ISO e identificar las categorías

Tenemos:

- Soporte y control: 27002, 27003, 27004, 27005
- Controles específicos para diversos sectores: 27010, 27011, 27013, 27015, 27017, 27019
- Auditoría y certificación: 27006, 27007, 27008, 27009
- Economía y gobernabilidad: 27014, 27016

NIST, y demás estándares referencia

- NIST: Dictamina estándares que aplican para los Estados Unidos (ver 800-61,)

-

Con las *rainbow tables* se pueden hacer ataques de fuerza bruta que permiten encontrar colisiones, si se encuentra la colisión se puede descifrar la contraseña. Las *rainbow tables* es la base de datos por las que comparamos hashes

Probablemente nos den una lista de hashes y debemos encontrar la contraseña y Jon de Ripper en linux opcrack

El NIST también emite certificados, por ejemplo en NIST 800-61 que trata sobre cómo reaccionar a incidentes. Tenemos que hacer lo mismo

El ISO y el NIST son diferentes en el tema de que ISO es internacional

Los frameworks nos permiten

Ejemplo, un banco que tiene presencia en otros países necesitará de servicios en la nube, así que hay que mantener el sistema que realiza las transacciones disponibles al 100% del tiempo.

Hay que alinear las medidas al negocio. Se necesita diseñar y utilizar sistemas de gestión. Evaluar los riesgos

El error no solo es de computadoras

La famosa capa 8, la persona, es el eslabón más débil, puede ser vulnerado fácilmente, por lo que se necesita mucha capacitación para las personas en el entorno. Un ejemplo muy famoso es el de Kevin Nip, algo que aseguraba que podía entrar a cualquier computadora sin hacer nada en el lado de ella.

NoB4 vende cursos de consciencia

- **Identificar**
- **Proteger**
- **Detección:** Contamos con herramientas como antivirus o elementos de monitoreo para saber cuando hay eventos, dependiendo del análisis de los eventos podemos determinar si se trata de un incidente
- **Responder**
- **Recuperar**

Se debe informar al INAI si hay incidentes por ley, y después se debe realizar la respuesta correspondiente

Como realizar un ataque

1. **Reconocimiento/Identificación:** (OSINT) Identificar la estructura que está expuesta de la organización
 - Realizar una auditoría, buscar información en redes, o deep-web
 - El reconocimiento es pasivo, es empaparnos de información
 - OSINT: Obtener
2. **Escaneo/Enumeración:** El escaneo nunca es pasivo. Tanto el escaneo como el reconocimiento son clave pues son las bases para poder desarrollar lo más posible el resto de etapas relacionadas con el ataque, si no 'reconocemos' algo, no podemos hacer algo con el

<https://securitytrails.com/blog/google-hacking-techniques>

198, 10, 127 son privadas.

Protegerse

- Las computadoras que cumplen distintos roles deben estar en distintas sub-redes, no pueden estar en la misma red máquinas de un administrador y de las personas de limpieza.
- Hay que tener sistemas de gestión para manejar las alertas que se reciben

Formas verbales en los estándares

- Shall: indica un requerimiento
- Should: recomendación
- May: Algo está permitido
- Can: Algo es posible

Estructura del ISO/IEC 27000:2018

1. Objetivo
2. Referencias normativas
3. Términos y definiciones
4. ISMS: Sistemas de gestión de la seguridad
5. Familia de estándares ISMS
6. Bibliografía

Detección de vulnerabilidades

La gestión y detección de vulnerabilidades son necesarias para poder realizar

Este tipo de acciones no solo aplican a lo relacionado a IT, sino que engloba toda la organización.

Un sistema de gestión es un conjunto de elementos para establecer objetivos que permitan

Todos los estándares de ISO están basados en el ciclo de Deming, de mejora constante

Comandos & Términos

- Vulnerabilidad: Debilidad de un activo que por definición puede ser explotada
- Amenaza: Todo aquello que puede explotar una vulnerabilidad
- Riesgo: Efecto de incertidumbre sobre los objetivos
- Análisis de riesgo: Proceso de comprender la naturaleza de riesgo y determinar su nivel
- Propietario del riesgo: Quien debe gestionar un riesgo
- Tratamiento del riesgo: Modificarlo, mitigarlo
 - Evitar
 - Aceptar
 - Mitigar
 - Transferir
- Gestión de riesgos: Aplicación sistemática de gestión de políticas, procedimientos y prácticas de actividades de comunicar, consultar, establecer contexto, analizar, evaluar, tratar, monitorear y revisar el riesgo.
- Control: medida que modifica un riesgo
- netstat -autopna: Muestra la actividad
- appliance: Una computadora/servidor que está dedicado a realizar una sola función. Por ejemplo tenemos un servidor que se usa para enviar actualizaciones a toda la org
- OSINT: Open Source Intelligence, búsqueda de información en fuentes abiertas
- activo: persona o

- IDS: Sistema de detección
- Matriz Raci: Es un arbol de responsabilidades
- Control: Modifica un riesgo

Aplicaciones

- En Wireshark captura todos los paquetes que encuentre el dispositivo en la red
- En NetworkMiner procesa todos los paquetes e identifica los dispositivos, su información, IP, etc.
- owasp (<https://owasp.org/>) tiene distintas herramientas de código libre, cada 4 años ve que vulnerabilidades encuentra la gente.

ISMS

Las responsabilidades de gestión de la información.

La seguridad suele ser un área pequeña del departamento de IT, lo que pasa cuando se implementa un ISMS la seguridad pasa de ser solo un sub área de IT a ser un departamento a parte, el Departamento de Dirección de Seguridad.

Dividido en Gestión, Pentesting, actualizaciones, diseño de políticas, centro de Operaciones de seguridad (SOC) donde se monitorea, responde, etc. Así como DevSecOps es una mezcla de DevOps y de seguridad, para proteger toda la cadena de *suministro*.

Hacer esto deja más acceso directo al CEO para reportar riesgos.

Cuando Seguridad se encuentra dentro de IT, se crea un conflicto porque la prioridad de IT es mantener siempre en funcionamiento los sistemas, no tanto la seguridad. Si el área de seguridad depende de TI se le da mucho más peso a la producción.

En el sistema de gestión permite prevenir y responder a incidentes porque se tienen procesos, políticas y herramientas.

Los sistemas de gestión de la seguridad de la información tienen base en calidad.

Tiene:

- Base regulatorias:
 -
- Catálogo de controles
 - Dominios
 - Generales

Es un proceso que involucra todas las áreas.

derechos *sarco*: Derecho, por ser dueños de nuestra información. Nos dan la facultad de elegir a quien darle nuestros datos personales y cuando quitárselos.

estas políticas deben estar documentadas, disponibles para quien lo necesite en la organización

Clausulas generales, la tiene todo sistema. Cambia el tema definiciones y eso

Particulares tienen lo mismo pero se orientan específico al tema a gestionar.

Control: Mitigar un riesgo, medidas que permiten mitigar un riesgo

Control se estructura por:

- Dominio: Procesos para la seguridad de la información, es un proceso. Ejemplo en el ISO está el proceso de políticas de seguridad las políticas se deben revisar una vez al año para ver si fue efectivo

Politica, tiene una estructura de sistema de gestion, muy similar.

De la politica general nacen las politicas especificas.

a partir de una politica se pueden establecer procesos de gestion, que involucran recursos

[Imagen de las flechas]

Un proceso da paso a la creacion de procesamientos, por ejemplo para escanear vulnerabilidades.

En el video es claro como la empresa tiene un sistema de monitoreo

Politica

De la politica general se derivan distintas politicas específicas. Establecer el sistema de gestión permite crear politicas > procesos > procedimientos. Hay que tener en cuenta que no todas las personas que lean el documento saben todos los terminos, por lo que es necesario explicarlo

• Politicas:

- **Proceso:** El proceso es lo que vamos a realizar, son como objetivos.
- **Procedimiento:** Son los pasos a realizar para cumplir el proceso, ya dentro del procedimiento se especifican las herramientas. El procedimiento es solo una parte del proceso
- **Capacitación:** Está involucrado en el sistema de gestión
- **Implementación de herramientas:** Está involucrado en el sistema de gestion

También es parte del sistema de gestión **operaciones/monitoreo, herramientas, appliances de seguridad.**

Ejemplo de Politica https://www.mtss.go.cr/perfiles/lineamientos_circulares_directrices_politicas_internas/lineamientos-circulares-directrices-politicas%20internas/DGAF-DTIC-OF-191-2020.pdf

Secciones:

- Alcance: Quién tiene que aplicar los contenidos de la politica
- Organigrama/Gobernancia
-

Cada país tiene una secretaría que permite acceder a las Normas ISO, por ejemplo, a mejor precio. Cada país tiene sus “normas” que son prácticamente la traducción, entonces cada país tiene su “propia” norma pero no se la inventó, la tradujo el país. No poner en documentos públicos marcas ni versiones

OWASP realiza una encuesta cada 4 años donde pregunta por la vulnerabilidades más comunes <https://owasp.org/www-project-top-ten/>

27001: Requisitos 27002: Controles

Ejemplo de Uber, en 15 de septiembre tienen un incidente y lo hacen saber por medio de Twitter, informan que avisarán.

Ahora vemos el caso de Uber, donde se inicia con las credenciales de un empleado de Uber, pudieron entrar a la intra-net, vulneran por medio de scripts en powershell, vulneran un servicio de credenciales y terminan con todas las credenciales.

Sin medidas de seguridad lo suficientemente robustas podemos terminar con incidentes, es importante tener sistemas de identificación y autenticación.

- Identificación: Capacidad de poder identificar de forma exclusiva a un usuario en un sistema, por ejemplo cuando queremos realizar una conexión. “Hola Pedro”
- Autenticación: Cuando se verifica que se ingresaron las credenciales correctas,
- SSO: Single Signed On, capacidad de autenticación que permite a los usuarios ingresar a múltiples servicios usando las mismas credenciales, se usa porque
 - Simplifica el acceso
 - Mejorar la seguridad
 - Controlar el acceso: Porque se realiza todo con el mismo sistema
 - Reducir llamadas a soporte: Porque solo hay 1 contraseña
 - Tiene ventajas desde el punto de vista de un administrador
- PAM: Monitoreo de acceso privilegiado, un *appliance*, por lo general en la nube, que permite administrar cuentas y accesos privilegiados, podemos configurar los permisos de forma que todos puedan ver solo lo que deben ver. Es necesario en la nube.
 - Permite restringir en base a localización (IP)
 - Descubrir cuentas privilegiadas
 - Asignar cuentas aleatorias a las cuentas que tenemos
 - Controlar el acceso a las cuentas privilegiadas, junto con cuentas de emergencia y compartidas (al estilo MySQL)
 - Aislar, monitorear, registrar/grabar, auditar comandos y sesiones

En el caso de uber aún así pudo conectarse por medio del PAM, que le dio acceso a las credenciales de los servicios

Control de acceso

En el caso de algo físico es poder acceder a un lugar, en cambio en ciberseguridad se abarca acceso a información, credenciales, servicios, etc.

Por ejemplo por teclado, credenciales, en red, reconocimiento facial, etc.

Politica de control de acceso

Tenemos que tener políticas de control de acceso. El 27002 indica que la política específica de control de acceso tiene que establecer, documentar y actualizarse en base a cómo se tiene que proteger la información. De forma que todos tengan acceso solo a lo que necesitan acceso.

Tenemos que tener sistemas bien desarrollados que permitan la creación y eliminación de usuarios de forma efectiva, y tener mecanismos de autenticación como:

- MFA: Multiple Factor Authentication que involucra celular, correo, aplicación, etc.
- SSO: Una sola credencial en todos lados
- Pueden ser dos o una sola
 - IAM: Manejo de identidades.
 - PAM: Monitoreo de aplicaciones.

Gartner es una consultoría que hace estudios de diversas herramientas, presentan su cuadrante mágico de las herramientas que evaluaron en distintos temas.

IAM

Las personas adecuadas pueden acceder a los recursos correctos en el tiempo correcto.

Tendencias Gartner

- Cómo hacer para no causar molestias a los usuarios legítimos

Etapas

- Reconocimiento
- Escaneo
 - Con escaneo pasivo se refieren a realizar el escaneo de la forma más silenciosa
- Acceso
- Mantener acceso
- Eliminar huellas

Arquitectura de seguridad

NIST es una organización de estado.

Una arquitectura de seguridad incorpora herramientas de seguridad perimetral

Criptografía

Involucra la confidencialidad, integridad (porque queremos que llegue íntegro) y la autenticidad

Viene de kryptos y grafos: Ocultar la escritura

El hash es una función que transforma de forma no reversible. Podemos usar hashes para verificar si un archivo ha sido modificado, pues dos contenidos diferentes alimentados a una función hash generará dos hashes diferentes.

Criptografía

Tiene distintos usos, por ejemplo:

- Cifrar mensajes/bases de datos
- Autenticación (firma electrónica)

Hash

Función que transforma de manera irreversible un mensaje

Kerberos

Cifrar cosas que pasan por la red

Active directory 0

Proporciona detalles de los privilegios de cada usuario, autentica pero no da el acceso a los recursos. Es un sistema de autenticación, evita el envío de contraseñas

Desventajas:

- Se tiene que migrar todas las contraseñas, por ejemplo de sistemas unix a kerberos
- Una persona podría acceder al servicio de tickets
- Las aplicaciones tendrán que llamar a kerberos. Implica estar dependiendo en todos lados en tener kerberos

Funcionamiento:

- Permite autenticar, en lugar de enviar en texto plano las credenciales se envía por medio del protocolo de kerberos
- Se envía un ticket, un paquete que devuelve un sustituto temporal

X.509

Tipo de certificado que se utiliza por ejemplo para el SSL de HTTP. Parte integral de la arquitectura PKI

Proveedor	Tipo de Certificado	Costo aproximado
-----------	---------------------	------------------

GoDaddy	Certificado SSL de validación de dominio (DV)	107.51 mxn/mes
Digicert	DigiCert Basic TLS/SSL Certificate	432.08 mxn/mes
HostGator	Positive SSL	40 mxn/mes

Podemos usar:

- OpenSSL: Firmado por nosotros mismos
- LetsEncrypt:

TLS es el sucesor de SSL, SSL está obsoleto.

Podemos realizar una prueba intentando acceder a recursos que no existen, que muestra versiones.

Podemos ver información sobre el certificado más a profundidad con SSL LABS, de global sign

- HSTS: Redirecciona consultas a los puertos seguros
- IDS : Detecta
- IPS : Detecta y bloquea

Herramientas

- SIEM: Security Information and Events
- SPLUNK: