FIPS PUB 200 y X.800

Jesus Erick Vera Callme •*jesus.vera@ucsp.edu.pe*

1 FIPS PUB 200

FIPS Publicacion 200: Minimos requisitos de Seguridad para informacion y la informacion Federal. Esta englobado dentro de la categoria "Seguridad de la Informacion".

Esta norma se refiere a la especificacion de los requisitos minimos de seguridad para los sistemas de informacion y de informacion federales.

Esta norma especifica los requisitos minimos de seguridad para la informacion federal y la informacion de sistemas en 17 areas relacionadas con la seguridad.

Esta ley fue promulgada por el Presidente en diciembre del 2002, reconociendo la importancia de la seguridad de informacion a los intereses enconomicos y de seguridad nacional de EEUU. Ley por la cual las agencias federales deben cumplir con la norma que asegura la seguridad minima para el cumplimiento de estandares mediante el uso de controles de seguridad cuarto.

El proposito principal de esta ley es que se reconozca la fundamental importancia de la seguridad de informacion dentro de una agencia federal con respecto a los intereses economicos y de seguridad nacional de EEUU.cuarto:

Los requisitos minimos de seguridad contemplan 17 areas relacionadas con la seguridad, y respecto a la integridad disponibilidad confidencialidad de los sistemas de informacion federales y la informacion procesada, almacenada y transmitida con motivo.{cuarto.

Las especificaciones para los requerimientos minimos son :

1. Control de Acceso: la organizacion debe limitar acceso al sistema de informacion a usuarios autorizados, procedimientos que actuen dentro de su limite de seguridad impuesto.
2. Capacitacion y sensibilización: la organizacion debe asegurar que administradores y usuarios de la organización de sistemas de información sean conscientes de los riesgos de seguridad asociados con sus actividades y de la las leyes, órdenes ejecutivas, directivas, políticas, normas, instrucciones, reglamentos o procedimientos relacionados con la seguridad de los sistemas de información de la organización.
3. Auditoria y rendicion de cuentas: las organizaciones deben crear, proteger y retener informacion de auditoria de sistemal registros en la medida necesaria para permitir el seguimiento, analisis e investigacion legal.
4. Certifacion, acreditacion y evaluciones de seguridad: las organizaciones debe evaluar periodicamente los controles de seguridad en los sistemas de informacion de la organizacion para determinar si los controles son eficaces en su solicitud. Implementar planes de acciones para corregir errores
5. Gestion de Configuracion: la organizacion debe establecer y mantener una linea de base de seguridad e inventariar sistemas de informacion organizacional.
6. Planificacion de la contingencia :la organizacion debe establecer mantener y efectivamente implementar planes para responsabilidad de emergencia, operaciones de recuperacion.
7. Identificacion y Autentificacion: la organizacion debe identificar infromacion de sistema, usuarios, procedimientos o dispositivos de autentificacion, debe verificar la identidad de los mismos, autentificar el acceso a informacion organizacional.
8. Respuesta a incidentes: la organizacion debe establecer una capacidad de manejo de incidentes operacionales, lo que incluye preparacion, analisis, deteccion y planeamiento.
9. Mantenimiento: las organizacion deben realizar un mantenimiento periodico y oportuno sobre la organizacion, proporcionar un control eficaz de las herramientas.
10. Proteccion de medios : la organizacion debe proteger informacion en papel como en digital, limitar su acceso, sea el caso destruir.
11. Proteccion fisica y del entorno: la organizacion debe limitar el acceso fisico a la informacion del sistema, equipos, entornos operativos a las personas autorizadas, proteger el entorno fisico que brinda apoyo a los sistemas de informacion.
12. Planeamiento: la organizacion debe desarrollar, documentar e implementar planes de seguridad para la informacion de la organizacion.

13. Seguridad Personal: las organizaciones deben garantizar que las personas que ocupan posiciones de responsabilidad dentro de las organizaciones (incluidos los proveedores de servicios de terceros) son dignos de confianza y conoce criterios de seguridad establecidos para esas posiciones

14. Evaluacion de Riesgos: las organizaciones deben evaluar periódicamente el riesgo para las operaciones de la organización (Incluyendo la misión, funciones, imagen o reputación), activos de la organización, y los individuos, como resultado de la operación de los sistemas de información de la organización y el procesamiento, almacenamiento o transmisión asociada de información de la organización.

15. Adquision de sistemas y servicios: las organizaciones deben asignar suficientes recursos a manera adecuada proteger los sistemas de información de la organización, deben garantizar los procesos del ciclo de vida de desarrollo de sistemas que emplean incorporar consideraciones de seguridad de la información, deben garantizar las restricciones de uso de software de empleo e instalación; y asegurar que los proveedores de terceros emplean medidas de seguridad adecuadas para proteger la información,

16. Proteccion de los Sistemas y comunicaciones: las organizaciones deben supervisar, controlar y proteger comunicaciones de la organizacion (informacion transmitida).

17. Integridad de sistemas e informacion: las organizaciones deben identificar, informar la correcta informacion y defectos del sistema de informacion para proporcionar proteccion contra codigo malicioso.

Los diecisiete áreas representan un programa de base amplia, equilibrada información de seguridad que se ocupa de la gestión, el funcionamiento y los aspectos técnicos de la protección de los sistemas de información y de información federales [3].

2 X.800 : Una arquitectura de Seguridad

Es un servicio dado por una capa de protocolo de comunicacion dentro de los sistemas abiertos , esto nos asegura el tener una seguridad adecuada de los sistemas o de sus transferencias de datos.segundo.

X.800 es una indicacion que nos da caracteristicas basicas que deben cumplir a fin de ser tratadas cuando se quiera conectar una red (computadoras entre computadoras) de acuerdo a su topologia (WAN,LAN).

Es una descripcion y no una especificacion de implementacion, de los servicios de seguridad basicos que pueden ser aplicados cuando es necesario proteger la interoperacion (comunicacion) que existe entre los diversos sistemas.

Dicha descripcion se define en que la capa del modelo de interconexion de sistemas abiertos se puede aplicar cada servicio e incluye los mecanismos que pueden ser implementados para ofrecerlos, asi como dar la administracion de seguridad.[1].
Estos servicios de seguridad brinda servicios para la autenticación, control de acceso, confidencialidad de datos, integridad de datos y no repudio que puede ejercer en el curso de las comunicaciones entre sistemas, entre los clientes y los sistemas, y entre los usuarios y los sistemas internos. Además, un conjunto de mecanismos de seguridad generalizados están definidos que son aplicables a cualquier comunicación (tales como la detección de eventos, gestión de registro de auditoría de seguridad y recuperación de la seguridad). X.800 va a centrarse en ataques de seguridad,mecanismos y servicios.[1]
X.800 se define en 4 categorías principales las cuales son:

1. Autenticación: Confirma que la identidad de una o más entidades conectadas a una o más entidades sea verdadera. Entiéndase por entidad un usuario, proceso o sistema. De igual forma corrobora a una entidad que la información proviene de otra entidad verdadera.

2. Control de acceso: Protege a una entidad contra el uso no autorizado de sus recursos. Este servicio de seguridad se puede aplicar a varios tipos de acceso, por ejemplo el uso de medios de comunicación, la lectura, escritura o eliminación de información y la ejecución de procesos.

3. Confidencialidad: Protege a una entidad contra la revelación deliberada o accidental de cualquier conjunto de datos a entidades no autorizadas.

4. Integridad: Asegura que los datos almacenados en las computadoras y/o transferidos en una conexión no fueron modificados. No repudio: Este servicio protege contra usuarios que quieran negar falsamente que enviaran o recibieran un mensaje.[2]

3 Conclusiones

References

[1] [Online], Disponible en. http://www.wirhanblog.com/2013/03/itu-x800.html.

[2] [Online],Disponible en. http://ataisminz.blogspot.pe/2013/03/the-x800-security-service.html.

[3] [Online],Disponible en. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.