Carrera de Computación

Título:

Análisis del NIST Serie 800

Asignatura:

Seguridad de la información

Estudiantes:

Adrián Viscaino

Bryam Barrera

Pedro Illaisaca

Docente:

Ing. Jennifer Yepez

Cuenca, 25 de octubre de 2021

Buenas prácticas, estándares y leyes para la Seguridad de la Información
Serie 800 de la publicación especial del NSIT

1. Antecedentes de la norma 800-Series SP800

Cada día de nuestra vida compartimos información personal con otras personas, ya sea por medio de aplicaciones, por medio de registros para tramites, transacciones bancarias, asuntos de salud, etc. Toda empresa e institución ese encuentra en la necesidad de almacenar y proteger la información de sus clientes o sus servicios debido a que actualmente es uno de los activos más valiosos, estos temas han provocado que surja un término conocido como "La seguridad en la información" que visto de manera breve no es más que las técnicas y gestiones que se hace para garantizar características de integridad, confiabilidad y disponibilidad de la información (Perez, 2021).

Para reconocer que información debe ser protegida debe cumplir con ciertas características: critica o una parte primordial para la empresa, valiosa para el giro de negocio y sensible para que se puedan manejar el acceso por roles (Perez, 2021).

Dentro de la seguridad de la información tenemos muchos documentos que establecen leyes y normas para la protección de los datos, en este documento de trata la norma SP800, en donde se trata de diferentes documentos que se pueden descargar libremente, estos son facilitados por el gobierno federal de los EE. UU y describen algunas de las políticas de seguridad informática además de prácticas y reglas. (NIST, 2018)

Esta serie también proporciona diferente información la cual cubre la gestión y practicas activas de seguridad de la información.

Documento	800 Series SP800
Creada	1990, actualmente se encuentra en su 5ta Versión.
Autor	Estados Unidos
División	Dividido en 166 documentos de libre descarga

2. Artículos o normativas relevantes para la Seguridad de la Información

Dentro de la serie “SP 800” existen documentos que contienen información relevante para el ámbito de buenas prácticas operativas en la seguridad de la información, algunos de los documentos más relevantes son:

NORMA	“SP 800-34"
TITULO	“Contingency Planning Guide for Federal Information Systems”
JUSTIFICACION	Dentro de este documento se pueden encontrar pautas, instrucciones y recomendaciones para la creación de planes de contingencia que permitan mantener un continuo servicio del sistema, tomando decisiones como la migración a un equipo externo, el traslado del equipo a otro punto o adoptando métodos manuales para algunas funciones del sistema (Swanson et al., 2010). Uno de los problemas de los sistemas de seguridad es que siempre deben garantizar el acceso y disponibilidad de su información, en base a esto es necesario definir planes para que cuando haya ciertas fallas en el sistema se pueda contar con medidas temporales hasta obtener una recuperación completa. Esto es importante ya que una empresa que presenta fallos en su infraestructura adquiere mala reputación y provoca pérdidas de clientes.

NORMA	“SP 800-41"
TITULO	“Guidelines on Firewalls and Firewall Policy”
JUSTIFICACION	Se considera firewall a cualquier tipo de tecnología que controle el tráfico de una red, este documento es una guía para las políticas que se debe manejar dentro de un firewall, centrándose en puntos como, crear políticas de entrada y salida del tráfico de red, identificar los requerimientos que se deben tomar en cuenta para escoger el firewall, crear las reglas para mejorar y personalizar el firewall, gestionar el firewall durante su funcionamiento (Scarfone & Hoffman, n.d.). Se considera este documento debido a que el firewall es uno de las primeras puertas de entrada a una red, de acuerdo a las necesidades de la empresa estos deben permitir o denegar el tráfico a los dispositivos de la empresa, de esta manera se evita que intrusos puedan colarse a la red por puertos abiertos y así mejorando los aspectos de seguridad de la empresa.

NORMA	“SP 800-44"
TITULO	“Guidelines on Securing Public Web Servers”
JUSTIFICACION	Entre los dispositivos más atacados están los servidores web, por ello este documento brinda normas y recomendaciones para la instalación y gestión de los servidores y su infraestructura, además de los ataques más comunes y las formas de contrarrestarlos (Tracy et al., 2009). Para una empresa que depende de sus servicios tecnológicos para estar en funcionamiento es vital que sus equipos siempre puedan estar activos y funcionales, por ello el seguir esta norma brindara soluciones a futuras fallas o ataques y el conocimiento de cómo actuar frente a fallos del servidor.

NORMA	“SP 800-45"
DESCRIPCION	“Guidelines on Electronic Mail Security”
JUSTIFICACION	En las empresas una de las formas más comunes de comunicación es el correo electrónico, debido a eso es uno de los puntos favoritos de los atacantes, al tener clientes estos pueden propagar malware a otros usuarios de manera involuntaria y por falta de conocimiento, por ello este documento busca brindar a las empresas asistencia al momento de instalar y configurar un servicio de correo electrónico, tratando temas como : implicaciones de seguridad en el correo electrónico, encriptaciones, filtrado de contenido, administración de servidores, etc. (Jansen & Scarfone, 2008) Las información contenida en este documento brinda pautas para que las empresas mejoren el uso de los correos electrónicos, esto implica poner restricciones a sus empleados para evitar situaciones de ataques provocados por descuido de ellos, o por compartir información peligrosa.

NORMA	"SP 800-50"
DESCRIPCION	"Building an Information Technology Security Awareness and Training Program"
JUSTIFICACION	Este documento presenta una guía para crear un programa de capacitación y concientización sobre S. I. , tratando temas como el diseño, tareas a identificar, desarrollo del material, implementación y post-implementación (Wilson & Hash, 2003). Este documento se toma en cuenta en aspectos de la S. I. debido a que la mejor estrategia para garantizar que la información este a salvo es que el personal conozca y se concientice de la importancia de estos planes, así se evita caer en ataques por engaños derivados de falta de conocimiento.

NORMA	"SP 800-61"
DESCRIPCION	"Computer Security Incident Handling Guide"
JUSTIFICACION	Una de las tareas más difíciles es poder tener una respuesta oportuna a ataques y fallos, debido a la demanda de recursos y planificación que esta lleva, en este documento se estudia los ataques más recientes y la manera en que se trataron, brindando a la empresa asistencia en el manejo de incidentes (Paul Cichonski, Tom Millar, Tim Grance, 2012). Cuando los usuarios se encuentran con fallos en un sistema y la indisponibilidad de los servicios, estos llegan a pensar que la información privada o no ha sido robada y por ello genera un grado de desconfianza muy alto, esto provoca pérdidas a la empresa y debe solucionar de manera oportuna los incidentes que se puedan dar para evitar ese tipo de situación.

NORMA	“SP 800-83"
DESCRIPCION	“Guide to Malware Incident Prevention and Handling for Desktops and Laptops”
JUSTIFICACION	El malware es uno de los códigos más intrusivos, destructivos y comúnmente transmitido por los usuarios, el recuperar un equipo que ha sido infectado es una tarea costosa y tediosa, por lo que este documento presenta normas para mejorar la capacidad de la empresa de responder a este tipo de incidentes, implementando políticas para solventar incidentes con malware, planes de prevención de ataques de malware, uso de arquitectura defensiva, etc. (Souppaya & Scarfone, 2013) Ingresar equipos infectados a una empresa de trabajo puede ser un daño muy grave a la empresa y a sus procesos de producción, por ello se debe contar con planes de respuesta a estas situaciones, para evitar la pérdida masiva de información y fallos de los equipos.

NORMA	“SP 800-88"
DESCRIPCION	“Guidelines for Media Sanitization”
JUSTIFICACION	El proceso de saneamiento de medios se refiere a tratar a los datos de manera que no puedan ser accedidos de manera fácil por un intermediario al momento de su envío y recepción, dentro de este documento se encuentran algunas recomendaciones para el saneamiento de datos basándose en la categorización de la información y el nivel de confidencialidad que se busca dar (Kissel et al., 2014). Al vivir en una época donde todo es comunicado por tecnología, las veces que enviamos información importante a otro punto está esta vulnerable a ataques y a que alguien pueda capturar lo que se envía, por ello es necesario añadir niveles de seguridad como encriptaciones para aumentar el nivel de complejidad de la captura de información por un tercero.

NORMA	"SP 800-92"
DESCRIPCION	"Guide to Computer Security Log Management"
JUSTIFICACION	El log en un sistema informático es un informe de los procesos que pasan y los resultados que se obtienen, dentro de los sistemas de seguridad también se generan log y este documento presenta algunas normas para la gestión de archivos log (Kent & Souppaya, 2006). Para incrementar el grado de fiabilidad de un sistema de información es necesario ir conociendo cómo se comporta, los problemas que ha tenido, para saber esto existen los archivos log que nos brinda una descripción más detallada de las distintas situaciones, por ello es un punto clave en un sistema de seguridad de la información.

NORMA	"SP 800-116"
DESCRIPCION	"Guidelines for the Use of PIV Credentials in Facility Access"
JUSTIFICACION	Este documento brinda pautas para el uso de tarjetas de verificación de la identidad, determinando las áreas de acceso, tecnologías de reconocimiento para autenticación como tarjetas biométricas, certificados de autentificaciones, llaves de acceso (Ferraiolo et al., 2018). El uso de este documento brindara a las empresas un enfoque para el uso de tarjetas de identificación como medio de autentificación, determinar los niveles de acceso y las tecnologías a usar es algo que se determinara de acuerdo al acceso a la información.

NORMA	“SP 800-122"
DESCRIPCION	“Guide to Protecting the Confidentiality of Personally Iddentifiable Information”
JUSTIFICACION	De acuerdo al giro de negocio uno de los valores más relevantes para una empresa son los datos de sus clientes, así que es importante encontrar formas de protegerla, este documento ofrece un enfoque basado en riesgos, este documento se desarrolló en base a leyes federales de EEUU, pero se puede adaptar a cualquier parte y sus leyes (McCallister et al., 2010). Algunas normas que se pueden encontrar son, las empresas deben saber que información tienen almacenada, las empresas deben hacer uso de la menor cantidad de información personal que le sea posible, se debe categorizar la información personal y así brindarle la seguridad necesaria, etc. Si para una empresa los datos de sus clientes son de un gran valor se deben adaptar todas las medidas de seguridad posible, al ser información tan sensible de terceros, su pérdida o daño puede traer graves consecuencias.

3. Prácticas de la norma 800-Series SP800

Sabemos que en la actualidad existen diferentes herramientas para proteger nuestra información y muchos usuarios que utilizan medidas para protegerse de cualquier tipo de riesgo llegando a aplicar estos estándares.

Casos o Ejemplos donde se debe o debían haber aplicado estos estándares.

Datos de ciudadanos ecuatorianos filtrados en una base en miami

En septiembre de 2019 una compañía dedicada a la seguridad informática “vpnMentor” encontró un servidor que era usado para el análisis de datos por una empresa, dicho servidor contenía datos de millones de personas ecuatorianas, dicho sea de paso, el servidor no contaba con ningún tipo de protección ya que podía ser accedido por cualquier persona con conocimientos intermedios en informática.

La compañía de seguridad indico que se descubrió este hallazgo en base a un procedimiento que consisten en realizar un mapeo web en conjunto con escaneo de puertos, de este modo es posible encontrar bases de datos abiertas (BBC News Mundo, 2019).

Para este tipo de escenario podemos considerar los problemas de cómo está almacenada la información recordando es considerada confidencial cualquier tipo de información de carácter personal

Ataque de Ransomware en Banco Pichincha.

En el presente año sucedió un ataque de ransomware donde se vieron afectados sus servicios en línea y cajeros automáticos, esto se llegó a saber gracias al trabajo de una industria de ciberseguridad los cuales habrían informado al sitio especializado Bleeping Computer de que este habría sido un ataque de ransomware con actores de amenazas que instalan una baliza Cobalt Strike en lo que sería la red.

Además, este sitio afirma que habría podido acceder a una notificación interna la cual se envió a las diferentes agencias del Banco Pichincha en donde se llegó a notificar a sus empleados de que estos problemas como las aplicaciones bancarias y los autoservicios no están en operación debido a un "problema tecnológico" (El Comercio, 2021)

Ciberataque a importante red de Estados Unidos

En el presente año se dio uno de los más grandes ciberataques a la mayor red de oleoducto en el país de Estados Unidos, el cual provoco que el gobierno de este declarara en estado de emergencia regional.

Se informo que un grupo de piratas informáticos llego a desconectar esta red por completo y pudo llegar a sustraer alrededor de más de 100GB de información sobre el Oleoducto Colonial el cual transporta un estimado de 2,5 millones de barriles por día.

Analistas de este mercado predicen que el precio de los combustibles podría llegar a aumentar entre un 2% y 3%, pero podría llegarse a dar un impacto más negativo si el apagón se prolongara por más tiempo.

Según Digital Shadows, la cual es una empresa de ciberseguridad ubicada en Londres la cual se dedica a rastrear a ciberdelincuentes globales comento que este ataque se produjo porque hackers encontraron como infiltrarse al sistema de este por la gran cantidad de ingenieros que ingresan al sistema de forma remota al control del oleoducto (BBC News Mundo, 2021).

Ataque informático a Corporación Nacional de Telecomunicaciones del Ecuador

En el presente año la corporación de telecomunicaciones CNT EP dio a conocer una denuncia ante la Fiscalía del Estado sobre un ataque a sus sistemas informáticos.

Se habría dado a conocer que el ataque es de tipo ransomware donde sus sistemas registraban anomalías llegando a tener intermitencias sobre lo que sería la atención al cliente, sus agencias y servicio de contacto (El Comercio, 2021).

Recomendaciones

Como recomendaciones se puede decir que estas prácticas pueden llegar a prestar una solución a cualquier cuestión al momento de plantearse de implementar un tipo de sistema de gestión para la seguridad en una empresa. Donde toda protección puede llegar a ser importante por lo más mínimo que sea, ya que el mínimo descuido que pueda llegarse a dar puede ocasionar una violación de los datos de esta.

Sugerencias de Mejora:

“Vetting the Security of Mobile Applications SP 800-163 Rev 1”: Este documento trata sobre la verificación de aplicaciones móviles mediante procesos en los que intervienen herramientas de terceros encargadas en definir si una aplicación es adecuada para su uso en una Organización, conforme con los requisitos de seguridad planteados (Quirolgico, Voas, Karygiannis, Michael, & Scarfone, 2015). Con el objetivo principal de mitigar vulnerabilidades de software y configuraciones incorrectas.

Entonces la sugerencia que se plantea para este documento es implementar el uso de Enterprise Mobility Management (EMM) ya que pone a disposición el uso de tecnologías, procesos y políticas para el desarrollo de aplicaciones en organizaciones, del mismo modo se sugiere tomar en cuenta a sistemas subyacentes como por ejemplo a aplicaciones de internet de las cosas (IoT) y por ultimo también es necesario tomar en cuenta la seguridad de comunicación entre servicios web y un servidor backend.

“Guidelines for Securing Wireless Local Area Networks (WLANs) SP 800-153": En este documento se hace mención a varias configuraciones con las que debe contar las redes inalámbricas IEEE 802.11 en organizaciones (Souppaya & Scarfone, 2012), pese a que es un documento que engloba muchas recomendaciones de configuración frente a ataques.

Se sugiere tomar en cuenta las desventajas de implementar el protocolo WPS ya que en determinados fabricantes tener este servicio habilitado conlleva a un riesgo de intrusión a la red de personal no autorizado.

“**Secure Virtual Network Configuration for Virtual Machine (VM) Protection SP 800-125B":** En este documento contempla en su mayoría parámetros de configuración de redes virtuales usadas en interconexión de máquinas virtuales organizadas en cuatro áreas las cuales son segmentación de red, redundancia de rutas, control de tráfico usando firewalls y monitoreo de trafico de las máquinas virtuales (Chandramouli, 2016).

Sin embargo, se sugiere tomar en cuenta aspectos de seguridad para las máquinas virtuales o conocidas como seguridad a nivel de host, donde los aspectos más importantes serian autenticación usando protocolos seguros, cifrado de datos, control de acceso y respaldos.

Referencias Bibliográficas

Chandramouli, R. (2016). *Secure Virtual Network Configuration for Virtual Machine (VM) Protection.*

Quirolgico, V., Voas, J., Karygiannis, T., Michael, C., & Scarfone, k. (2015). *NIST Special Publication 800-163.*

Souppaya, M., & Scarfone, K. (2012). *Guidelines for Securing Wireless Local Area Networks.*

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. Polo del conocimiento, 2(12), 145-155.

Bonilla Guerrero, J. V. (2021). Análisis de seguridad de la información aplicando la metodología NIST SP 800-30 y NIST 800-115 para la Empresa Textiles JHONATHEX (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos).

BBC News Mundo. (2019). Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano. [online] Available at: www.bbc.com/mundo/noticias-america-latina-49721456

El Comercio. (2021). Ataque ransomware, que utiliza una baliza Cobal Strike, habría provocado caída de servicios en Banco Pichincha, afirma portal de ciberseguridad. [online] Available at: www.eluniverso.com/noticias/ecuador/ataque-ransomware-que-utiliza-una-baliza-cobal-strike-habria-provocado-caida-de-servicios-en-banco-pichincha-afirma-portal-de-ciberseguridad-nota/

BBC News Mundo. (2019). EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país. [online] Available at: https://www.bbc.com/mundo/noticias-internacional-57033536

El Comercio. (2021). CNT apaga todas sus computadoras tras fuerte ataque informático. [online] Available at: www.elcomercio.com/actualidad/negocios/cnt-ataque-informatico-ransomware-fiscalia.html

NIST. (21 de 05 de 2018). *NIST*. Obtenido de https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

Perez, A. (06 de 09 de 2021). *OBS Business School*. Obtenido de https://www.obsbusiness.school/blog/seguridad-de-la-informacion-un-conocimiento-imprescindible

Ferraiolo, H., Mehta, K., Ghadiali, N., Mohler, J., Johnson, V., & Brady, S. (2018). NIST Special Publication 800-116 Revision 1 Guidelines - Guidelines for the use of PIV credentials in facility access. *NIST Special Publication*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-116r1.pdf

Jansen, W., & Scarfone, K. (2008). Guidelines on Cell Phone and PDA Security Recommendations of the National Institute of Standards and Technology. *NIST Special Publication 800-124*, 51.

Kent, K., & Souppaya, M. (2006). Guide to Computer Security Log Management. *Nist Special Publication*.

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). NIST Special Publication 800-88 (Revision 1) Guidelines for Media Sanitization. *NIST Special Publication 800-88, 800*, 16–27. http://dx.doi.org/10.6028/NIST.SP.800-88r1%0Ahttp://abouthipaa.com/wp-content/uploads/NIST-Special-Publication-800-88_Guidelines-for-Media-Sanitization_SP800-88_rev1.pdf%5Cnhttp://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

McCallister, E., Grance, T., & Kent, K. (2010). Guide to protecting the confidentiality of personally identifiable information (PII). *Special Publication 800-122 Guide*, 1–59.

Paul Cichonski, Tom Millar, Tim Grance, K. S. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, *800–61*, 79. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Scarfone, K., & Hoffman, P. (n.d.). Guidelines on Firewalls and Firewall Policy Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*.

Souppaya, M., & Scarfone, K. (2013). NIST Special Publication 800-83 Revision 1 - Guide to Malware Incident Prevention and Handling for Desktops and Laptops. *NIST Special Publication*, *800*, 83. http://dx.doi.org/10.6028/NIST.SP.800-83r1%0Ahttp://dx.doi.org/10.6028/NIST.SP.800-83r1%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. *NIST Special Publication 800-34 Rev. 1*, *May*, 150.

Tracy, M., Jansen, W., & McLarnon, M. (2009). Guidelines on Securing Public Web Servers. *NIST Special Publication*, *800*, 44. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44.pdf

Wilson, M., & Hash, J. (2003). Nist Sp 800-50. *Nist*, *October*, 70.