SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN BAJO LA PLATAFORMA DE ISERIES Y CÓMO MANEJAR ADECUADAMENTE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Joaquín Javier Sierra Nieto
Universidad Piloto de Colombia
Bogotá – Colombia
Ingjjsierra@gmail.com

Resumen— Los incidentes de seguridad de la información en las organizaciones actualmente están creciendo de forma muy rápida por tal razón es importante que la detección de un ataque cibernético en una organización sea lo más rápido posible, porque en ocasiones un ataque puede durar días, meses e incluso años. Lo importante en la estrategia de seguridad es que la respuesta sea rápida y eficiente. Cuando hablamos de un impacto en el negocio y no sólo en el área de TI, nuestro nivel de seguridad será más maduro y por tanto nuestro nivel de visibilidad y respuesta será mayor. Por tal razón en este documento se establece un modelo de buenas prácticas para el manejo y tratamiento de un incidente de seguridad de la información basándose en los mejores estándares como la NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), tomando como base los lineamientos y recomendaciones de la norma ISO IEC 27001 – 2013 para la plataforma de iSeries.

Índice de Términos— Plataforma de iSeries, Servicios, incidente de seguridad, estándares.

Abstract— The Incidents of information security in organizations are currently growing very quickly for that reason it is important that the detection of a cyber attack in an organization as fast as possible because sometimes an attack can last for days, months and even years. What is important in the security strategy is that the response is quick and efficient. When we talk about an impact on the business and not just in the IT area, our security level will be more mature and therefore our visibility and response will be higher. For this reason in this paper a model of good practice for the management and treatment of a security incident information based on the best standards such as NIST (National Institute of Standards and Technology is established - (Computer Security Incident Handling Guide) based on the guidelines and recommendations of the ISO 27001 - 2013 for the iSeries platform

I. INTRODUCCIÓN

En la actualidad todas las organizaciones, independientemente de su tamaño, son conscientes de la importancia de tener implantadas una serie de políticas de seguridad tendientes a garantizar la continuidad de su negocio en el caso de que se produzcan incidencias, fallos, actuaciones malintencionadas por parte de terceros, pérdidas accidentales o desastres que afecten a los datos e informaciones que son almacenados y tratados, ya sea a través de sistemas informáticos. Por lo tanto, es importante que la información que reside en las organizaciones e independiente al core del negocio que esta se dedica, en ocasiones no se presta la debida atención necesaria a sucesos que ocurren sobre ella o en el peor de los casos no son conscientes del valor importante que esta tiene dentro de sus organizaciones. Desafortunadamente, en la actualidad los sistemas de información son los objetivos principales de los atacantes. Para generar daños irreparables. Por tal razón, la respuesta a este problema es un sistema de gestión aplicada a la seguridad de la información (SGSI), que tiene como objetivo mantener siempre los riesgos por debajo de unos umbrales asumidos por la propia organización.

Para esto es necesario, implementar herramientas que permitan analizar y ordenar la estructura de los sistemas de información, establecer procedimientos de trabajo para definir la seguridad y disponer de controles que permitan medir la eficacia de las medidas de seguridad implementadas, sin olvidar que todo esto se debe revisar periódicamente, realizando mejoras constantemente y

siempre bajo las directrices de una política de seguridad definida por la organización. ¿Pero todo esto es necesario en las organizaciones?, ¿Realmente se encuentra en peligro los sistemas de información de ciberataques? la respuesta es siempre sí. Todas las organizaciones y especialmente en aquellas en donde existe una motivación económica están expuestas tanto externa como internamente a sufrir ataques de diferente naturaleza como los son: virus, daño de imagen, sabotaje, beneficio económico, fuga de información, fallos técnicos, errores humanos, fuego, inundación, entre otros, son algunas de las amenazas a las que una organización está expuesta. La originalidad de esta propuesta en primer lugar es dar a conocer un modelo de gestión de incidentes de seguridad de la información desde un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información bajo la plataforma de iSeries. El resto de este trabajo se organiza de la siguiente forma.

En primer lugar, se describe, la sesión I, introducción. En la sección II, seguridad de iSeries 400, en la sección III, Modelo de gestión de incidente, en la sección IV, recomendaciones después de cumplir las etapas, sección V, conclusiones.

II. SEGURIDAD DE ISERIES 400

A. Arquitectura AS/400

El AS/400 es un sistema integrado muy complejo que incluye el hardware, el software, la seguridad, una base de datos y otros componentes. La arquitectura avanzada AS/400 es única en que es extremadamente adaptable y puede incorporar fácilmente nuevas tecnologías. Esto es importante en mercado rápido de hoy de la computadora que cambia. El AS/400 se diseña para separar el software y el hardware así que los cambios en uno tienen poco efecto en el otro. Esto se logra a través del interfaz de la máquina (MI) que es un interfaz de la programación de software entre el uso, el sistema operativo y el hardware. El MI es un interfaz de programación de uso completo (API) fijó que todos los usos deben utilizar para conseguir a al hardware. Éste es cómo el AS400 alcanza la independencia del software. [1]

B. Sistema Operativo OS/400

El sistema operativo para el AS/400 se llama OS/400. El OS/400 reside sobre el MI. Esto permite que el sistema operativo sea independiente del hardware. La mayoría de los componentes del sistema operativo manejan funciones tales como memoria, proceso, programa, y gerencia de I/O. En el AS/400 estas funciones de nivel inferior son manejadas por el código interno licenciado (LIC) que es el software de sistema operativo debajo del MÍ. El LIC protege programas de uso y OS/400 contra cambios del hardware. Así otra vez, guardando el software a parte del hardware. [1]

C. Seguridad de ISeries

IBM propone algunos Consejos y herramientas de seguridad para la plataforma de iSeries [1]:

• *Niveles de contraseña:* Ofrece cifrado de seguridad por contraseña mejorado. Se da soporte a múltiples niveles de seguridad por contraseña utilizando algoritmos criptográficos avanzados para proteger las contraseñas de usuario.

• *Servicio de Autenticación de Red:* El Servicio de Autenticación de Red (NAS) es una herramienta que verifica la identidad de un usuario de una red. NAS autentica el usuario y, seguidamente, pasa la identidad autenticada a otros servicios de la red.

• *Firmas digitales:* La mayoría de programas del sistema operativo van firmados digitalmente. El valor del sistema. Puede utilizarse para evitar que se almacenen en su sistema programas no firmados o programas con una firma errónea. También se ha añadido soporte que le permitirá firmar sus programas, el archivo de salvar y los archivos continuos.

• *Red privada virtual (VPN):* La VPN nativa en OS/400 le permite proteger de forma selectiva sus aplicaciones de Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP).

• *Filtrado de paquetes de Protocolo Internet (IP):* Proporciona la capacidad de bloquear el tráfico de IP de forma selectiva, basándose en la información de las cabeceras de los paquetes IP y las específicas del protocolo.

• *Firewall para iSeries 400:* El firewall para iSeries 400 (5769–FW1) es un producto software que habilita al Integrated Netfinity Server para iSeries 400 en el iSeries para que realice las funciones de un cortafuego. El cortafuego separa la red interna (protegida) de una red externa (no protegida) (generalmente Internet). Puede ejecutar el IBM Firewall para iSeries 400 en su sistema iSeries de producción (para proteger tanto su sistema de

producción como otros sistemas conectados). Para obtener la máxima protección de seguridad, por lo general deberá utilizar un sistema iSeries dedicado y separado como servidor internet. También puede elegir ejecutar el cortafuego en un sistema iSeries multiuso que ejecute las aplicaciones de producción y que proporcione servicios de internet. No obstante, el éxito de esta implementación depende en gran medida tanto del diseño de la aplicación como de la meticulosidad de sus normas de configuración.

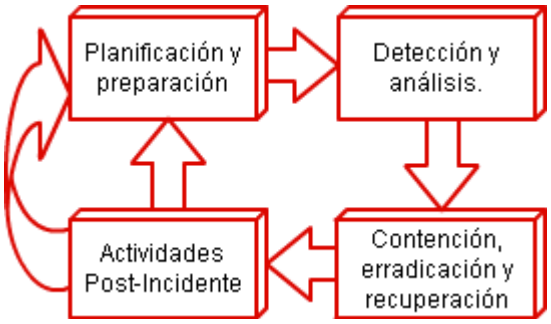
Todos estos concejos y herramientas de seguridad que propone IBM son de gran ayuda para evitar fugas de información. Pero resulta que un programa informático se considera seguro cuando cumple los cuatro pilares de la seguridad informática que son: confidencialidad, integridad, disponibilidad, autenticidad. Pero los incidentes de seguridad de información están a la orden del día por tal razón se propone en este documento unos lineamientos básicos para poner en marcha cuando se presente un incidente de seguridad de la información en las plataformas de iSeries. A través de un modelo propuesto, el cual está concebido para que se puedan integrarse a los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren. Cabe resaltar que en este modelo se basa en las mejores prácticas y documentos de uso libre por parte de la NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), tomando como base los lineamientos recomendados en norma la ISO IEC 27001 – 2013 numeral 16 de la misma, para la gestión de incidente.

III. MODELO DE GESTIÓN DE INCIDENTE

El objetivo de este modelo en primera instancia es permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada y minimizar los impactos adversos de los incidentes en la organización y sus operaciones de negocios mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente esto tiene como objetivo incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, lo que mejoraría el esquema global de la gestión de incidentes de seguridad de la información.

Como primera medida se establecerán, las etapas fundamentales de un modelo de gestión de incidente de tal forma que permitirá a las organizaciones estar preparadas para afrontar cada una de las etapas y adicionalmente definiendo responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Para definir las actividades de cada etapa se incorporan componentes definidos por la NIST y alineados con los requerimientos normativos de la NTC–ISO–IEC 27001-2013.

Fig. 1 muestra el modelo para manejar un incidente de seguridad de la información de las plataformas de iSeries [5].



A. DEFINICIÓN FORMAL DE LAS ETAPAS PARA LA GESTIÓN DE INCIDENTES

• *Definición de un incidente*

El instituto nacional de estándares y tecnología (NIST) define un incidente de la siguiente manera: " Una violación o amenaza inminente de violación de las políticas de seguridad informática, las políticas de uso aceptable, o prácticas de seguridad estándar. Un incidente también puede ocurrir en un nivel físico, en el que una persona tener acceso físico no autorizado a un área por cualquier medio. Por tal razón La organización de destino debe tener diferentes categorías y niveles para los diferentes tipos de incidentes. [3]

• Etapa 1 planificación y preparación

Esta etapa dentro del ciclo de vida de respuesta a incidentes suele hacerse pensando no sólo en crear un modelo que permita a la entidad estar en capacidad de responder ante estos, sino también en la forma como pueden ser detectados, evaluados y gestionar las vulnerabilidades para prevenirse, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros. En esta etapa el grupo de gestión de incidentes o quien se designe para esta labor debe velar por la disposición de los recursos de atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo de vida del mismo, creando (si no existen) y validando (si existen) los procedimientos necesarios y programas de capacitación.

La etapa de preparación debe ser apoyada por la dirección de tecnologías de la información o quien haga sus veces, incluyendo las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones por ejemplos. [2]

1) Gestión de Parches de Seguridad: las entidades dependiendo de su estratificación deben contar con un programa de gestión de vulnerabilidades (Sistemas operativos, bases de datos, aplicaciones, otro Software instalado), este programa ayudara a los administradores en la identificación, adquisición, prueba e instalación de los parches.

2) Aseguramiento de plataforma: Las entidades dependiendo de si estratificación deben ser aseguradas correctamente. Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos.

3) Seguridad en redes: Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS o IPS deben encontrarse al día. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.

4) Prevención de código malicioso: Todos los equipos de la infraestructura (Servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas de actualización al día.

5) Sensibilización y entrenamiento de usuarios: Usuarios en la entidad incluidos los administradores de TI deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad.

Las actividades descritas anteriormente buscan prevenir la ocurrencia de incidentes de seguridad de la información que esta soportada por TI, y adicionalmente es necesario realizar una evaluación mensual. [2]

• Etapa 2 detección, evaluación y análisis

A. detección

En este atapa gracias a los indicadores que son los eventos que nos señalan que posiblemente un incidente ha ocurrido generalmente algunos de estos elementos son [2]:

- Alertas en sistemas de seguridad.
- Caídas de servidores.
- Reportes de usuarios.
- Software antivirus dando informes.
- Otros funcionamientos fuera de lo normal del sistema

La identificación y gestión de elementos que alertan sobre un incidente nos proveen información que puede alertarnos sobre la futura ocurrencia del mismo y preparar procedimientos para minimizar su impacto. Algunos de estos elementos pueden ser:

- Logs de servidores.
- Logs de aplicaciones.
- Logs de herramientas de seguridad.
- Cualquier otra herramienta que permita la identificación de un incidente de seguridad.

En la entidad debe existir un listado de fuentes generadoras de eventos que permitan la identificación de un incidente de seguridad de la información.

B. Análisis.

Las actividades de análisis del incidente involucran otra serie de componentes, es recomendable tener en cuenta los siguientes:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.
- Los administradores de TI deben tener conocimiento total sobre los comportamientos de la Infraestructura que están Administrando.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).
- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones

de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.

• Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) ya que esto facilita la correlación de eventos y el análisis de información.

• Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.

• Crear matrices de diagnóstico e información para los administradores menos experimentados [2].

C. *Evaluación*

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad. La severidad del incidente puede ser:

• *Alto Impacto:* El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del instituto. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

• *Medio Impacto:* El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

• *Bajo Impacto:* El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

D. Clasificación De Incidentes De Seguridad De La Información

Algunos ejemplos de clasificación de incidentes podrían ser (esta clasificación está sujeta a cada entidad dependiendo de su infraestructura, de sus riesgos y criticidad de los activos. La clasificación dada es solo un ejemplo [2]:

• *Acceso no autorizado:* Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.

• *Modificación de recursos no autorizado:* Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.
• *Uso inapropiado de recursos:* Un incidente que involucra a una persona que viola alguna política de uso de recursos.

• *No disponibilidad de los recursos:* Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.

• *Multicomponente:* Un incidente que involucra más de una categoría anteriormente mencionada.

• *Otros:* Un incidente que no puede clasificarse en alguna de las Categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías.

E. Priorización De Los Incidentes Y Tiempos De Respuesta

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación) se debe determinar el nivel de prioridad del mismo, y de esta manera atenderlos adecuadamente según la necesidad. A manera de ejemplo se definen una serie de variables que podrán ser utilizadas para realzar la evaluación de los incidentes [2]:

• *Nivel de Prioridad:* Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

• *Impacto Actual:* Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

• *Impacto Futuro:* Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

F. Tiempos de Respuesta

Para el caso de la atención de incidentes de seguridad se ha establecido unos tiempos máximos de atención de los mismos, con el fin de atender adecuadamente los incidentes de acuerdo a su criticidad e impacto. Los

tiempos expresados que a continuación se van describir son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso [4]:

Niveles de prioridades – tiempos de respuestas

• Inferior - 3 horas

• Bajo - 1 hora

• Medio - 30 minutos

• Alto - 15 minutos

• Superior - 5 minutos

Cabe resaltar que cada entidad está en la libertad de definir tiempos de atención a incidentes como crean conveniente [2].

• Etapa 3 contención erradicación y recuperación

Es importante para la entidad implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Esta fase se descompone claramente en tres componentes:

A. Contención

Esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones, por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son [2]:

• Criterios Forenses.

• Daño potencial y hurto de activos.

• Necesidades para la preservación de evidencia.

• Disponibilidad del servicio.

• Tiempo y recursos para implementar la estrategia.

• Efectividad de la estrategia para contener el incidente (parcial o total).

• Duración de la solución

B. Erradicación y recuperación

Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

En algunas ocasiones durante el proceso de atención de incidentes de seguridad informática específicamente en la fase de “Contención, Erradicación y Recuperación” se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema [2].

• Etapa 4 actividades post-incidente

Las actividades Post-Incidente básicamente se componen del reporte apropiado del incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores [2].

IV. RECOMENDACIONES DESPUÉS DE CUPLIR LAS ETAPAS

Una de las partes más importantes de un plan de respuesta a incidentes de TI es la de aprender y mejorar. Cada equipo de respuesta a incidentes debe evolucionar para reflejar las nuevas amenazas, la mejora de la tecnología, y las lecciones aprendidas. Mantener un proceso de "lecciones aprendidas" después de un incidente grave, y periódicamente después de los

incidentes menores, es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes mantener un adecuado registro de lecciones aprendidas permite conocer:

• Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.

• Los procedimientos documentados.

• Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.

• Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.

• Acciones correctivas pueden prevenir incidentes similares en el futuro.

• Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

El proceso de lecciones aprendidas puede poner de manifiesto la falta de un paso o una inexactitud en un procedimiento y son un punto de partida para el cambio, y es precisamente debido a la naturaleza cambiante de la tecnología de la información y los cambios en el personal, que el equipo de respuesta a incidentes debe revisar toda la documentación y los procedimientos para el manejo de incidentes en determinados intervalos [2].

V. CONCLUSIONES

• El propósito de este artículo fue recomendar un modelo de buenas prácticas para el manejo y tratamiento de un incidente de seguridad de la información para las plataformas de iSeries basándose en los mejores estándares, para esto se definió inicialmente el nivel de protección que estos ofrecen, cuáles son sus herramientas de seguridad y las debilidades y fortalezas que esas herramientas poseen.

• Para la realización de este modelo se utilizaron como apoyo metodológico una serie de estándares que ya están avalados y usados en el mundo, estos determinaron no solo los elementos de seguridad a evaluar y las herramientas a utilizar, sino que además se convirtieron en una guía para su correcta aplicación, garantizando que los resultados obtenidos fueran los más completos y los más rigurosos para minimizar el riego de un incidente de seguridad.

• Gran parte del análisis del modelo propuesto no presentaron demasiadas dificultades en el proceso de establecer las etapas y se puede concluir que, si las organizaciones no manejan un modelo de buenas prácticas para el manejo y tratamiento de un incidente de seguridad de la información en las plataformas de iSeries. No es por su nivel de complejidad, sino simplemente por no tener conciencia de los impactos que este puede generar.

• Al realizar el modelo de las buenas prácticas para el manejo y tratamiento de un incidente de seguridad en las plataformas de iSeries, se puede mejorar de forma significativa la seguridad de esta plataforma, ya que si se aplica el modelo de forma correcta, se puede presentar una reducción en el número de vulnerabilidades detectadas y lograr minimizar el número de incidentes de seguridad, lo que podríamos construir un sistema más seguro evitando así los incidentes de seguridad de información.

REFERENCIAS

[1]. (2016) La página web de IBM. [En línea]. Disponible: http://www.ibm.com/eserver/iseries/infocenter

[2]. (2016) La página web de Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia [En línea]. Disponible: http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Incidentes.pdf.

[3]. (2016) La página web de NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide) [En línea]. Disponible: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

[4]. (2016) La página web de ISO. [En línea]. Disponible: http://www.iso.org/iso/catalogue_detail?csnumber=54534

[5]. (2016). J. J Sierra Nieto, **"**Modelo para manejar un incidente de seguridad de la información bajo las plataformas de iSeries**"**.