Gestión Integral de Seguridad de Infraestructuras críticas paralas organizaciones locales alineadas a las Normas IRAM ISO IEC 27.001 y 27002.

Mag. Licenciada Mirta Elizabeth Navarro[1] Mag. Abogado María del C. Becerra[2],
marisabecerra2005@yahoo.com.ar, mirthaenavarro@yahoo.com.ar

Abstract.: Con esta propuesta de gestión integral diseñada para la protección de la información alineada a la norma IRAM ISO IEC 27001, 27002 y a lastendencias y normas de seguridad informática, consistente en la creación y adopción de un marco regulatorio que favorezca la identificación y protección de las infraestructuras estratégicas y críticas de la U.N.S.J., se favorecerá la colaboración entre los diversos sectores públicos y privados, para el desarrollo de estrategias y estructuras adecuadas para la protección de los activos de información. Todo ellodará real importancia a la nueva visión del estado, liderada por la incorporación de las TIC´s en los procesos administrativos y bajo el sustento de la comunicación íntegra y confidencial necesaria en el entorno globalizado de e-gobierno, se busca dar impulso a la administración electrónica.

Keywords: Gestión Integral de seguridad. Infraestructuras críticas. Propuesta para implementar el plan Infraestructuras críticas y ciberseguridad.

1 Introducción

Para ayudar a garantizar una gestión de integral de las infraestructuras críticas[3] de las empresas se tomaron en cuenta dos normas de la familia de las normas ISO 27000 adaptadas y traducidas en nuestro país, especialmente las Normas IRAM ISO 27.001[4] y 27002[5] y su antecedente 17799), en base a ellas se definieron los requisitos para el sistema de gestión de seguridad (SGSI) propuesto.

En el proyecto "Convergencia de Tecnologías informáticas y Metodologías para la implementación de sistemas de Información"se analizaron las políticas, prácticas, procedimientos y estructuras organizacionales como conjunto de controles necesarios para implementar un sistema de gestión para las infraestructuras críticas.

En Argentina por Resolución 580/2011 se crea, en el ámbito de la Oficina Nacional de Tecnologías de Información de la subsecretaria de Tecnologías de Gestión de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros, el "Programa Nacional De Infraestructuras Criticas De Información y Ciberseguridad" en el marco de lo establecido la Ley de Ministerios (t.o. Decreto Nº 438/92), a fin de impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras

[1]Licenciada en Administración de empresas egresada de la U.N.S.J. Magíster en Gestión de Organizaciones egresada de la Universidad de Valparaíso. Chile. Docente de la U.N.S.J. Directora del Proyecto Convergencia de Tecnologías informáticas y Metodologías para la implementación de Sistemas de información

[2]Abogado, egresado de la UCC. Magíster en Informática egresado de la Universidad Nacional de la Matanza. Docente Investigadora de la U.N.S.J. Directora del Instituto de informática del Foro de Abogados de San Juan

[3]Las infraestructuras críticas son aquellas instalaciones, redes, equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto en el bienestar de los ciudadanos o en el eficaz funcionamiento del gobierno. Las infraestructuras críticas están presentes en numerosos sectores: financiero, transporte y distribución, energía, salud, comunicaciones, y administraciones públicas.

[4] En Argentina es IRAM, como organismo nacional de normalización, quien la estudia a través del Subcomité de Seguridad de la Información y la adopta como IRAM-ISO/IEC 27001. Se publica bajo el nombre Tecnología de la información. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos, difundiéndola en la región a través de cursos y seminarios.

[5]Aprobada y consensuada por el IRAM (Instituto de Normalización Argentino) en el año 2002

estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones.

El "Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad" no interceptará ni intervendrá en conexiones o redes de acceso privado de acuerdo a lo estatuido por la Ley Nº 25.326 de Protección de los Datos Personales y su Decreto Reglamentario Nº 1558 del 29 de noviembre de 2001.

El programa de ICIC, tendrá a su cargo los siguientes objetivos:

a) Elaborar y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito del Sector Público Nacional.

b) Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante, fortaleciendo lazos entre los sectores público y privado; haciendo especial hincapié en las infraestructuras críticas.

c) Administrar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional que hubieren adherido al Programa y encausar sus posibles soluciones de forma organizada y unificada.

d) Establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.

e) Investigar nuevas tecnologías y herramientas en materia de seguridad informática.

f) Incorporar tecnología de última generación para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Nacional.

g) Asesorar a los organismos sobre herramientas y técnicas de protección y defensa de sus sistemas de información.

h) Alertar a los organismos que se adhieran al presente Programa sobre casos de detección de intentos de vulneración de infraestructuras críticas, sean estos reales o no.

i) Coordinar la implementación de ejercicios de respuesta ante la eventualidad de un intento de vulneración de las infraestructuras críticas del Sector Público Nacional.

j) Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten los organismos del Sector Público Nacional que hubieren adherido.

k) Centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas del Sector Público Nacional que hubieren adherido al Programa y facilitar el intercambio de información para afrontarlos.

I) Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.

m) Promover la coordinación entre las unidades de administración de redes informáticas del Sector Público Nacional, para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad.

n) Elaborar un informe anual de la situación en materia de ciberseguridad, a efectos de su publicación abierta y transparente.

ñ) Monitorear los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como Infraestructura Crítica para la prevención de posibles fallas de Seguridad.

o) Promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, las Organizaciones de Gobierno, al público en general, como así también del rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica.

p) Difundir información útil para incrementar los niveles de seguridad de las redes teleinformáticas del Sector Público Nacional.

k) Interactuar con equipos de similar naturaleza.

II.-Gestión integral de la seguridad.

A los efectos de garantizar la selección de controles de seguridad adecuados y proporcionales y para proteger la información crítica de las organizaciones se eligieron las Normas IRAM ISO IEC mencionadas porque se consideran recomendables para cualquier empresa grande o pequeña en cualquier parte del mundo y para aquellos sectores que tienen información crítica o gestionan la información de otras empresas.

Para protegerse de estas amenazas la British Standards Institution publicó en 1995 la norma BS 7799 - parte 1 y 2- que sirvió como antecedente a ISO para el estudio de dos estándares internacionales adoptados y reconocidos a nivel mundial: la norma ISO/IEC 17799:2000 Information technology - Security techniques - Code of practice for information security management, revisada en 2005 y reemplazada por la ISO/IEC 27002, que establece los requisitos fundamentales a tener en cuenta para establecer, operar, controlar, revisar, mantener y mejorar un sistema de gestión de seguridad de la información. La norma 27.002 establece un conjunto de reglas de normalización de los conceptos y operatorias de seguridad informática.

Tal cual lo enfatizan los autores, la seguridad de la información se logra implementando un conjunto adecuado de controles que abarca políticas, practicas, y procedimientos, estructuras organizaciones y funciones del software. Estos controles deben ser establecidos para garantizar que se logren los objetivos específicos de seguridad de la organización".

La edición 2000 de esta norma fue publicada por IRAM dando como resultado la IRAM-ISO/IEC 17799:2002. Ésta fue estudiada por el Subcomité de Seguridad de la Información de IRAM (revisión de la IRAM 17798 cuyo antecedente es la BS 7799-2).

La norma está basada en el mismo modelo de los sistemas de gestión de la calidad de la familia ISO 9000. Establece conceptos similares sobre Requisitos de la documentación: alcance, política de seguridad, enfoque sistémico de identificación y valoración de riesgos, operaciones para el tratamiento de los riesgos, objetivos de control, controles y aplicabilidad de los mismos.

Actualmente para certificar un Sistema de Gestión de la Seguridad implementado bajo la norma ISO/IEC 17799 (ISO 27002) se utiliza la norma ISO/IEC 27001: 2005.

Tal como lo prevé la Norma IRAM ISO IEC 27.001 para una adecuada gestión de la seguridad de la información se propone implantar en las organizaciones locales un sistema que aborde esta tarea de una manera metódica, documentada y basada en objetivos claros de seguridad y en una evaluación de los riesgos a los que está sometida la información de las organizaciones locales.

En la práctica esta norma se presenta embebida en varias normativas estatales en Argentina. Forma parte de reglamentaciones de organismos del Estado para cumplir con diversos procedimientos, entre los que se destaca la comunicación A4609 del BCRA (Banco Central de la República Argentina). Un decreto del Poder Ejecutivo de la Secretaria de la Función Pública (2006) instaló la norma con el nombre de Sistema de Gestión de Seguridad del Estado. Existen 400 organismos estatales que la implementan pero no la certifican.

La comunicación A-4609 del Banco Central de la República Argentina[6], resulta así aplicable al conjunto de entidades del sistema regulado por dicha institución y establece los "Requisitos mínimos de gestión implementación control de los riesgos relacionados con la tecnología informática, sistemas de información y recursos asociados para entidades financieras".

En el apartado referido a la Gestión de seguridad la comunicación establece que las entidades financieras deben considerar en su estructura organizacional un área para la protección de los activos de información, con el fin de establecer los mecanismos para la administración y el control sobre el acceso lógico y físico a sus distintos ambientes tecnológicos y recursos de información: equipamiento principal, plataforma de sucursales, equipos de departamentales, subsistemas o módulos administradores de seguridad de los sistemas de aplicación, sistemas de transferencias electrónica de fondos, base de datos, canales de servicios electrónicos, banca por Internet y otros.

Por la complejidad de la implementación de la Norma, sería conveniente que la Administración Pública definiera de manera sistemática el alcance el proyecto, principalmente en las áreas de CONTROL DE ACTIVOS Y SEGURIDAD DE LOS RECURSOS HUMANOS.

Adoptar una norma de gestión de la seguridad de la información garantiza la correcta consideración de los activos de información de una organización junto con el análisis de su vulnerabilidad y amenazas, también asegura que se establezcan controles de procedimiento y tecnológicos (gestión de accesos mediante registro de huellas, control de información por Internet y mails, controles sobre el software y las bases de datos). Mediante la norma estos procedimientos se desarrollan de manera ordenada, pautada y controlada; no como simples impulsos aislados, sino como un verdadero sistema que garantice la confidencialidad, integridad y acceso a la información de gestión, de dirección, y pública de la empresa.

A partir de la generalización de la tecnología de la información y la comunicación proliferaron las situaciones de riesgo para los sistemas de información, las bases de datos y los recursos de hardware, a los cuales denominamos activos de la información.

[6]B.O. 31.156,16/05/2007, corregida por la Comunicación C-48.583/2007 BCRA y actualizada por la Comunicación B-9042/2007 BCRA

Se tomó en cuenta la decisión administrativa 669/2004 que estableció que los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8º de la Ley Nº 24.156 y sus modificatorias deberán dictar o adecuar sus políticas de seguridad. Conformación de Comités de Seguridad en la Información. Funciones de los mismos y responsabilidades en relación con la seguridad.

Los comités deberán integrado al menos por un miembro del Directorio o autoridad equivalente, y el responsable máximo del área de Tecnologías Informática y sistemas.

III.- Infraestructuras críticas.

Infraestructuras Criticas son las infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales". Se refiere tanto a empresas del sector TIC, agua, energía, industria nuclear, sistema financiero o transporte, ente otras.

Las Infraestructuras Criticas, son consideradas un conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación, siendo menester dictar medidas para la protección de tales infraestructuras.

Existen gran variedad de formas de ataque a los sistemas, con el fin de obtener esta información. Pero también existen políticas y paradigmas de seguridad actuales que nos permiten poner una brecha a estos ataques y proteger este recurso tan valioso.

Tomando en cuenta que el mundo contemporáneo se caracteriza por los profundos cambios originados en el desarrollo y difusión de las tecnologías de la información y la comunicación en la sociedad, las cuales se encuentran sustentadas en gran medida en el ciberespacio. Y que la utilización de las comunicaciones virtuales es un recurso que depende de la infraestructura digital, la cual es considerada como infraestructura crítica, entendiéndose ésta como imprescindible para el funcionamiento de los sistemas de información y comunicaciones, de los que a su vez dependen de modo inexorable, tanto el Sector Público Nacional como el sector privado, para cumplir sus funciones y alcanzar sus objetivos.

En el planteamiento de los instrumentos de planificación, se detectaron cambios estratégicos de protección que hasta ahora estaban enfocados principalmente a la seguridad física y que, ahora, como no podía ser de otra manera tienen un enfoque integral y actual de protección de las Infraestructuras críticas como conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra infraestructuras y garantizar la integración de estas actuaciones.

Se requiere un planteamiento de seguridad holístico (física, lógica, personal y operativa) de verdadera Seguridad Integral = Protección + Prevención donde la Gestión de riesgos debe ser su protagonista más importante y las soluciones pasen por la Evaluación de Impactos, establecimiento de Planes de contingencia, Planes de continuidad del negocio y de las operaciones y la determinación de los Sistemas y aplicaciones de garantía de alta disponibilidad.

En la Protección de Infraestructuras Críticas, es preciso estudiar los criterios que permitan determinar qué factores confieren carácter crítico a una infraestructura o elemento de infraestructura particular. Los criterios de selección deberían basarse en conocimientos sectoriales y generales. Pueden definirse tres factores de identificación de una infraestructura crítica potencial:

• Alcance - la pérdida de un elemento de infraestructura crítico se mide por el tamaño del área geográfica que pudiera verse afectada por su pérdida o indisponibilidad.

• Magnitud - el grado del impacto o de la pérdida puede evaluarse como nulo, mínimo, moderado o principal. Entre los criterios que podrían utilizarse para evaluar la magnitud potencial se encuentran los siguientes:

(a) impacto público (cantidad de población afectada, pérdidas de vidas, enfermedades, lesiones graves, evacuación);

(b) económico (efecto PIB, volumen de pérdida económica y/o degradación de productos o servicios);

(c) ambiental (impacto en el lugar y sus alrededores);

(d) interdependencia (con otros elementos de infraestructura críticos).

(e) político (confianza en la capacidad de las administraciones públicas);

Efectos en el tiempo - estos criterios determinan en qué plazo (tiempo) la pérdida de unelemento podría tener un impacto. En caso de sufrir un ataque, las estructuras críticas, causarían gran impacto en la seguridad, tanto física como económica del país. Este impacto se mide según unos criterios horizontales que determinan la

criticidad de una infraestructura. Se han establecido tres: el número potencial de víctimas, el impacto económico y el impacto público**.**

En la República Argentina se enuncia que El Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) tiene como finalidad impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías.

También impulsa una Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Información y la Comunicación (ENTIC) en Hogares y Personas, que permite contar con información desde la perspectiva de los usos y accesos de los hogares y de las personas a dichas tecnologías en la Argentina. La ENTIC se administró a todos los hogares para la Encuesta Anual de Hogares Urbanos (EAHU), cuya estimación se extiende al total de la población residente en hogares particulares urbanos, en localidades de 2.000 o más habitantes.

Mediante el Programa Nacional de Infraestructura Crítica de Información y Ciberseguridad (ICIC) e Internet Sano

- Se promoverá la concientización de la protección de las infraestructuras críticas de información y la ciberseguridad dentro de las dependencias del Sector Público Nacional, brindando asistencia técnica a los organismos nacionales, provinciales y municipales que lo requieran.
- Se actualizará la Estrategia Nacional ICIC.
- Se dictarán talleres y charlas técnicas sobre Ciberseguridad.
- Se formularán ejercicios de respuesta a incidentes.
- Se creará la Política de Seguridad de la Información.
- Se generarán nuevos contenidos para concientización de la ciudadanía.
- Se desarrollarán exposiciones y conferencias de concientización.
- Se concertarán alianzas público-privadas para la creación y difusión de contenidos.

Organismo responsable: Subsecretaría de Tecnologías de Gestión. Jefatura de Gabinete de Ministros. Fecha tentativa: diciembre 2013

IV. Propuesta para implementar en la UNSJ.

La Universidad Nacional de San Juan (U.N.S.J.) ha desarrollado una plataforma tecnológica a través de la cual se registra, procesa, transmite y almacena información mediante diferentes activos de Información, que permiten interactuar con la comunidad académica, ciudadanía en general y el personal universitario de todo el país, y como además se reconoce que la información que posee es un bien estratégico para sus fines, por lo que se requiere que sea protegida también su obtención, procesamiento, transmisión y almacenamiento. Considerando que la Resolución 580/2011 crea, el "Programa Nacional De Infraestructuras Criticas De Información y Ciberseguridad" en el marco de lo establecido la Ley de Ministerios (t.o. Decreto Nº 438/92), a fin de impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran. Dado que las universidades nacionales como órganos académicos deberían adherirse a lo previsto por la resolución 580/2011 que se creó, en el ámbito de la Oficina Nacional de Tecnologías de Información de la subsecretaria de Tecnologías de Gestión de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros, el "Programa Nacional De Infraestructuras Criticas De Información y Ciberseguridad" en el marco de lo establecido la Ley de Ministerios (t.o. Decreto Nº 438/92), se impone para la U.N.S.J. la obligación de establecer una Política de Seguridad que fije las directrices generales que oriente la materia de seguridad dentro de cada Unidad.

Para ello se crearía un comité que será el responsable máximo del área de Tecnologías Informática y sistemas. Y que deberá dictar o adecuar sus políticas de seguridad de la Universidad Conformación de Comités de Seguridad en la Información. Funciones de los mismos y responsabilidades en relación con la seguridad.

El encargado de seguridad de los activos de información debería establecer un organigrama de funciones, determinando la cantidad de miembros de la Unidad, cargos y funciones (discriminando quienes son los administradores de seguridad y/o miembros del comité). Tendría además a su cargo el desarrollo y actualización de las políticas de seguridad y controlar su implementación, utilizando como referencia las

Normas IRAM ISO 27.001[7] y 27002[8] y su antecedente 17799) debido a que en base a ellas se definieron los requisitos para el sistema de gestión de seguridad (SGSI) propuesto.

Para ello sería necesario para ello adoptar las medidas para la protección de la Infraestructuras críticas donde se fije entre otras cosas, la necesidad de que para esta gestión se fije:

- Un Plan de Seguridad del Operador (PSO)
- Un Plan de Protección Especifico (PPE) para cada una de las infraestructuras que haya sido identificada como critica por la Secretaria de para la Protección de Infraestructuras Criticas.

El encargado de seguridad debería recoger los contenidos mínimos que deben articular estos planes, y desarrollar un nuevo documento en el que se describe el modo de abordar la implantación de las medidas y más tarde reflejarlo en dichos planes.

Se entiende por incidente de seguridad todo incidente que impida el normal funcionam8ento de los activos de información y que afecte la Seguridad Informática.

La gestión de incidentes de Seguridad tiene por objeto restaurar la operación normal de los sistemas con tanta rapidez como sea posible y mitigar el impacto adverso a sus procesos, asegurando así que se mantenga debidamente la confidencialidad, integridad y disponibilidad de la información de la U.N.S.J.

El comité de Seguridad Informática definirá las pautas a seguir en la gestión de incidentes de seguridad, lo que deberán ser implementados por el Departamento de Sistemas de la U.N.S.J. bajo la coordinación del encargado de Seguridad de los activos de información.

Además deberá elaborar una Guía aplicativa del sistema de seguridad utilizando como apoyo la Norma IRAM ISO IEC 27001.

Se propone un sistema de gestión de Incidentes de seguridad porque es la forma en que la Organización dirige y controla aquellas actividades asociadas a la seguridad. De una manera más amplia debería contar con dos grandes apartados alineados con la estructura del Plan de Seguridad del Operador (PSO) y del Plan de protección Específico (PPE):

- Un capítulo dedicado al análisis de riesgos, uno de los aspectos principales de los mencionados planes.

Dos capítulos dedicados a recoger las medidas de seguridad lógicas y físicas que se deberán:

- Construir y proponer una normativa de seguridad aplicable al entorno local mediante la
- Implementación de un Equipo de Respuesta a Incidentes para la Universidad Nacional de San Juan.

La Metodología propuesta para el Manejo de Incidentes CSIRT[9] – UNSJ, básicamente se ha estructurado de acuerdo al siguiente esquema:

Cada uno de los pasos propuestos se describe a continuación:

1. Preparación y Protección

La fase de preparación consiste, principalmente, en la implementación de un equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), las actividades propuestas, que se deben realizar en esta fase son:

- Planificación del CSIRT – UNSJ
- Implementación del CSIRT – UNSJ
- Evaluación y funcionamiento del CSIRT
- Lecciones Aprendidas.

A más de definir un proceso de implementación de un equipo de CSIRT, es importante tomar en cuenta la Protección de la infraestructura de la Universidad para de esta manera asegurar que los sistemas, redes y aplicaciones tengan un nivel de seguridad adecuado. Las actividades de esta fase se realizan en conjunto con

[7] En Argentina es IRAM, como organismo nacional de normalización, quien la estudia a través del Subcomité de Seguridad de la Información y la adopta como IRAM-ISO/IEC 27001. Se publica bajo el nombre Tecnología de la información. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos, difundiéndola en la región a través de cursos y seminarios.

[8] Aprobada y consensuada por el IRAM (Instituto de Normalización Argentino) en el año 2002

[9] Un **Equipo de Respuesta ante Emergencias Informáticas** (**CERT**, del inglés **Computer Emergency Response Team**) es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

el área de Seguridad, pero básicamente el área de Manejo de incidentes tiene a su cargo la prevención de ataques, y si estos suceden mitigar el impacto. El área de seguridad realiza actividades de protección, en cuanto a configuraciones y garantiza la infraestructura informática de la Universidad.

2. Detección de Incidentes de Seguridad

Esta fase está compuesta de varias actividades, tales como: detección de incidentes, análisis inicial y documentación del incidente y tiene como objetivo la búsqueda de toda posible señal de ocurrencia de un incidente. Todas las actividades e información generada en esta fase en enviada al proceso de Triage, haciendo uso de los reportes establecidos.

La Detección de incidentes es un proceso que permite identificar las actividades inusuales que pueden comprometer la misión del CSIRT, consiste en la detección y evaluación de posibles incidentes, determinar si un incidente ha ocurrido, y de ser así, el tipo, extensión y magnitud del problema.

Estas actividades se pueden identificar de manera reactiva y proactiva.

Los incidentes se pueden detectar a través de muchos medios tales como: IDS basados en red

(NIDS) y en host (HIDS), software antivirus, software de control de integridad de archivos, sistemas de monitoreo de red, analizadores de logs, etc.

Los incidentes también pueden ser detectados por medios manuales, tales como reportes de incidentes de usuarios.

En el proceso de detección están involucrados: Encargado de Seguridad, CSIRT-UNSJ, Gestión de

Servicios TI, Infraestructura de TI, usuarios que han sido víctimas de algún ataque y otras áreas, incluye los siguientes aspectos:

- Señales de un incidente
- Detección de incidentes mediante la utilización de herramientas
- Detección de incidentes mediante el reporte de terceros.

Señales de un Incidente:

En el proceso de detección, la información sobre potenciales incidentes, vulnerabilidades, información de seguridad informática o de manejo de incidentes, puede ser obtenida de dos maneras:

- Detección Reactiva

Un incidente puede haber ocurrido o estar ocurriendo en este momento, puede ser detectado de varias maneras:

- El antivirus detecta que un equipo está contaminado con algún tipo de virus.
- Incidentes en el servidor web
- Envío de alertas y notificaciones por parte de otras organizaciones.
- Detección Proactiva
- Monitoreo de Red
- Escaneo de vulnerabilidades
- Investigación
- Análisis de Riesgos

La detección de incidentes es un proceso que permite saber si el sistema está en peligro o si los servidores corren el riesgo de detener sus servicios.

Esta actividad va de la mano con la detección proactiva, se debe tomar en cuenta el personal que se encargue del monitoreo y detección de actividad sospechosa, análisis de logs, uso de software de detección de intrusos, para cada una de estas actividades se deben tomar en cuenta los procesos establecidos en el Área de Seguridad para estas actividades.

Todos los datos analizados y los considerados sospechosos se envían al proceso de Triage.

Detección de incidentes mediante el reporte de terceros va de la mano con la detección reactiva, el usuario notifica del incidente al área de Gestión de Servicios, si el incidente se encuentra en la base de conocimiento de esta área, es atendido por ellos, caso contrario se envía el reporte del incidente al equipo CSIRT – UNSJ, en donde, primeramente se verifica que sea un incidente de seguridad.

Los incidentes que se envían al CSIRT-UNSJ y los que se atienden, son los que constan en la Categorización de incidentes del CSIRT-UNSJ.

- Análisis de Incidentes de Seguridad

En este proceso se busca analizar cada reporte de incidentes presentado, tanto por los usuarios y por los reportes obtenidos de las herramientas utilizadas, con la finalidad de verificar si realmente se trata de un incidente de seguridad, o son falsos positivos.

Se debe recalcar que el equipo CSIRT debe trabajar rápidamente en el análisis y validación de los incidentes, todas las acciones realizadas deben ser documentadas.

Uno de los mecanismos que sirve de soporte para Detección es la documentación del incidente, se han definido varios formatos para el reporte y respuesta de incidentes y vulnerabilidades, el uso de reportes ayuda a:

- Proveer información completa de un incidente al equipo
- Organizar la información recibida
- Priorizar reportes

La información que se solicita en el reporte de incidente es:

- Información de contacto
- Fecha de reporte
- Sistemas afectados
- Descripción del incidente
- Observaciones

A más de los reportes de incidentes, parte de la documentación incluye un documento en el que se detalla el cómo los usuarios deben realizar el reporte de los incidentes al equipo, etc.

Adicional al reporte de incidente enviado por el usuario, por parte del Equipo CSIRT-UNSJ se debe enviar un documento de respuesta a incidentes, en el que se detalle la información relativa a la atención y respuesta del incidente reportado, dependiendo del tipo de incidente, esta información será enviada a autoridades, y personal que requiera de esta información. (Esta sección, se detalla en la fase de la respuesta a incidentes).

En cuanto a los recursos humanos, es necesario que el plantel de empleados sea idóneo para la realización del trabajo de la Organización, pero además debe definir y comunicar sus funciones y responsabilidades.La misma organización debe establecer las necesidad información y facilitar y evaluar la eficacia de la formación y de esto debe haber evidencia (Es decir, se exige un registro de capacitación del personal y en lo posible la formación de una tablero de comando al efecto).

También se debe sensibilizar a toda la organización sobre la importancia de la capacidad humana de la Organización descansa sobre la formación que da a todos sus empleados. La organización dispone un potencial que debe ser aprovechado para poder subsistir y este es el potencial humano para ello se debe implantar los siguientes aspectos motivación, adiestramiento y Comunicación.Implantar en las infraestructuras críticas para mejorar los niveles de protección integrales.

Se propone crear un CSIRT dentro de la UNSJ, ello es un proceso que involucra un cambio estructural, organizacional y desde luego requiere de mucho esfuerzo y compromiso a todos los niveles. Sin duda un CSIRT viene a darle un gran valor a la organización ya que provee un punto de contacto único para afrentar, resolver y proponer en el campo de las nuevas tecnologías.

La protección del ciberespacio requiere de una organización que sirva de centro nacional decoordinación para asegurar y proteger el ciberespacio, cuya misión incluye vigilancia, alerta,respuesta y recuperación, con la colaboración de las entidades gubernamentales en los ámbitosnacional, estatal y local, el sector privado, el sector académico y la comunidad internacional.

Los principales objetivos que debe cubrir este centro nacional son:

Desarrollar un sistema nacional de seguridad y respuesta ante incidentes cibernéticos paradetectar, prevenir, responder y recuperarse de incidentes en el ciberespacio.

- Establecer un centro de coordinación para la gestión de incidentes cibernéticos que reúnen los elementos críticos del gobierno y los elementos esenciales de las infraestructuras de los operadores y los proveedores para reducir el riesgo y la gravedad de los incidentes.
- Participar en la vigilancia, alerta y mecanismos de intercambio de información.
- Elaborar y probar los planes de respuesta de emergencia, procedimientos y protocolospara asegurar que los colaboradores gubernamentales y no gubernamentales puedanfomentar la confianza ypuedan coordinarse de manera eficaz en caso de crisis.

La implementación del CSIRT-UNSJ permitirá:

- Contar con un equipo capacitado para la atención de incidentes brindando servicios proactivos, reactivos y de aseguramiento de la calidad en temas de seguridad de la información.
- Concientizar a la comunidad universitaria y usuarios finales sobre los riesgos y beneficios del uso de internet, pero, sobre todo de la importancia de tomar en cuenta las medidas de seguridad adoptadas en la Universidad.

Por otra parte como objetivo fundamental el construir y proponer una normativa de seguridad aplicable al entorno local, la implementación del equipo permitirá compartir la experiencia y resultados obtenidos con otras universidades.

Los beneficiarios de la implementación de este proyecto serán principalmente la UNSJ y con la implementación del proyecto:

- Otras Universidades, con la finalidad de profundizar y proponer temas de investigación.
- Organizaciones públicas y privadas que mantienen Equipos de Seguridad.
- Empresas y profesionales que brindan servicios de atención de incidentes.
- Participación efectiva de todos los intervinientes en el proyecto.

Hasta la fecha la participación de los integrantes del equipo se ve reflejada en el cumplimiento de las actividades, estas se han realizado acorde a lo planificado.

Se ha involucrado a personal de Marketing para la publicidad del CSIRT.

Se han realizado reuniones de Coordinación

Se mantuvieron reuniones con:

- Grupo de seguridad para la presentación de la metodología para el manejo de incidentes.
- Grupo de Administradores para comunicarles la existencia del CSIRT-UNSJ, uso de reportes de incidentes y políticas.

Se realizaran actividades de Difusión mediante emisión de boletines con tips de seguridad para usuarios, los mismos que se emitirán mensualmente. Como estrategia de marketing, durante el primer mes se emitirán boletines semanalmente, con el objetivo de posicionar el CSIRT-UNSJ en la comunidad universitaria.

- En conjunto con el área de marketing de la UNSJ se está preparando unaestrategia de comunicación para realizar la difusión del CSIRT-UNSJ, lo que incluye boletines informativos, notas periodísticas, etc.
- Emisión de un boletín sobre el CSIRT-UNSJ al área de marketing para que sea difundido a nivel interno en la UNSJ

Finalmente la guía deberá incluir un Anexo dedicado a la protección de los sistemas de monitorización y control de procesos e infraestructuras, dada su relevancia en este tipo de infraestructuras, así como un apartado en el que se recogen, de manera exhaustiva, todas las referencias utilizadas.

V. Conclusiones

La seguridad de la infraestructura digital se encuentra expuesta a constantes amenazas, que en caso de materializarse pueden ocasionar graves incidentes en los sistemas de información y comunicaciones, por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas.Los riesgos se han incrementado y sofisticado y hay una demanda de mayor eficacia que exige nuevas respuestas que requieren tecnología, eficacia y calidad. Eficacia y calidad que deben ser percibidas por el usuario.

La propuesta para gestión integral de la seguridad de la información diseñada para la protección de la información de las organizaciones locales, basada en las tendencias, normas de seguridad y estándares actuales y la creación y adopción de un marco regulatorio que favorecerá la identificación y protección de las infraestructuras estratégicas y críticas de la U.N.S.J. , promoverá la colaboración entre los distintos sectores y propiciara el desarrollo de estrategias y estructuras adecuadas para la protección de los activos de información de las organizaciones locales.

El proyecto de Creación e Implementación de un CSIRT Académico para la Universidad Nacional de San Juan, tiene como objetivo fundamental, el construir y proponer una normativa de seguridad aplicable al entorno local, la implementación del equipo permitirá compartir la experiencia y resultados obtenidos con otras universidades Nacionales con el objetivo de proponer la creación de una red nacional de CSIRTs académicos y contribuir así a la investigación y desarrollo de metodologías y buenas prácticas que permitan mejorar la seguridad de las redes.

Así hemos de concluir en que, sin duda hoy la responsabilidad y respuesta de una única Seguridad con mayúscula, integral e integrada, pública y privada, es estrictamente necesaria e irreversible.Por todo ello, para un adecuado presente y futuro hay que integrar el sistema de gestión de la Seguridad Pública y la Seguridad Privada hacia una nueva visión común y especial cultura de seguridad sobre la base de las amenazas complejas y la interdependencia e incrementar los recursos de análisis y liberarlos de viejas patologías y rigideces para desarrollar el esquema de Gestión Integral e Integrada de la Seguridad.

VI.-Referencias

31"Evaluación y Seguridad de un Sistema de Información", por José Alfredo Jiménez
http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml

32. "Administración segura de la información: Una experiencia de vinculación entre un ente del estado provincial y la U.N.P.A". Javier Díaz, L.I.N.T.I. – Universidad Nacional de La Plata
http://www.ing.unp.edu.ar/wicc2007/trabajos/ISBD/066.pdf

33. "Propuesta para un modelo de gestión de documentos electrónicos de archivo en la administración pública"- documento de trabajo elaborado por Carlos Alberto Zapata y Nelson Javier Pulido para el comité de gestión de documentos del sistema nacional de archivos

34.http://www.slideshare.net/scarchivistas/propuesta-para-un-modelo-de-gestin-de-documentos-electrnicos-de-archivo-en-la-administracin-pblica

Gómez Vieites, Álvaro (2007). Enciclopedia de la Seguridad Informática.

3.5Altmark, Daniel Ricardo y Molina Quiroga Eduardo. Tratado de Derecho Informático. Tomo III. Publicado por la Ley año 2012