Seguridad de la Información en los Proyectos Satelitales de Venezuela

Information Security in Venezuelan Satellite Projects

Christian A. Ledezma, PI-4 PASO 2, ABAE

[1]***Resumen*** **-El progresivo crecimiento de La Agencia Bolivariana para Actividades Espaciales (ABAE) implica un alto desarrollo de información, la cual pasa a formar parte importante como bien intelectual de la agencia y en donde la información y la tecnología de carácter espacial se convierten en propiedad de la Nación una vez procesada por el capital humano de la ABAE. Por tal motivo se están desarrollando políticas para el manejo de la seguridad de la información en los proyectos satelitales de la agencia a través de la implementación de estándares internacionales y del métodos de PDCA para atacar las vulnerabilidades y afrontar los riesgos que atañen a la información con carácter sensible y que con una mala Institución podría traer problemas de índole legal para la agencia o para la nación debido a los convenios y tratados internacionales que se llevan a cabo en el área de tecnología espacial.**

Palabras claves**- Información confidencial, SGSI, Seguridad de la Información.**

Abstract -The progressive growth of the Bolivarian Agency for Space Activities (ABAE) implies a high development of information, which becomes an important part of the intellectual good of the agency and where information and technology of a spatial nature become property of the Nation once processed by the human capital of the ABAE. For this reason, policies are being developed for the management of information security in the satellite projects of the agency through the implementation of international standards and PDCA methods to attack vulnerabilities and address the risks related to information with sensitive character and that with a bad Institution could bring legal problems for the agency or for the nation due to international conventions and treaties that are carried out in the area of space technology.

Index Terms- Confidential information, ISMS, Information Security.

I. INTRODUCCIÓN

LOS sistemas informáticos permiten la digitalización de la información reduciendo el espacio ocupado, facilitando el análisis, aumentando la rapidez del procesamiento y mejorando la presentación de la información. Generalmente, contienen gran cantidad de información confidencial y no confidencial que son fundamentales para la agencia y deben ser protegidos tanto de amenazas internas, como externas, por tal motivo la seguridad informática se aplica para garantizar que el material y los recursos de software se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto. Por lo cual deben aplicarse políticas para el desarrollo e implementación de la seguridad de la información en los proyectos espaciales que la agencia desarrolla [1].

La información, en todas sus formas (automatizada o no automatizada, formalizada o no formalizada, pública o reservada, etc.), es uno de los principales activos de la ABAE y necesaria para el normal funcionamiento y consecución de los objetivos, es por ello que deben existir políticas en seguridad de la información para proteger los activos y asegurar que estén disponibles cuando se necesiten, que sean fiables y que su distribución esté controlada. Esta necesidad se ve incrementada por el hecho de la cantidad de información que se maneja, dificultando los esfuerzos para su protección a medida que la ABAE se desarrolla en el campo espacial [2].

Es por ello, las políticas de seguridad de la información deben estar enmarcadas preferiblemente bajo el estándar ISO/IEC 27001, el cual define, alcanza y mantiene unos niveles apropiados de integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad de la información.

II. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

La Ley de Infogobierno define la Seguridad de la Información como:

"*Condición que resulta del establecimiento y mantenimiento de medios de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la información no autorizada, o que afecten la operatividad de las funciones de un sistema de computación, bajo los principios de confidencialidad, integridad, privacidad y disponibilidad de la información*" [3].

La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

- Crítica: Es indispensable para la operación de la agencia.
- Valiosa: Es un activo de la agencia de gran importancia.
- Sensible: Debe ser conocida por las personas autorizadas.

En términos más simples se resume como confidencial cuando es sólo para uso interno de la agencia y sus empleados, y no confidencial cuando es para ser difundida al público en general o al país.

C.A, Ledezma, ABAE, Venezuela (cledezma@abae.gob.ve)

A. *Tipo de Información que Requiere Seguridad*

El tipo de información que maneja la agencia es de diversa índole pero especialmente los conocimientos técnicos, prototipos, dibujos de ingeniería, software, procedimientos de pruebas, manuales de operación, resultados de pruebas eléctricas o mecánicas de modelos satelitales, modelos de ingeniería espacial, herramientas y equipos, sistemas y especificaciones de satelitales, instalaciones y sistemas de seguridad: así como contratos internacionales, datos financieros, datos comerciales, entre otros [4], es la información que la agencia necesita proteger a través de políticas para el uso apropiado de la información.

B. *Propiedades de la Seguridad de la Información*

La seguridad de la información (SI) busca que la información sea manejada según los criterios de autenticación, la integridad y la confidencialidad dentro de la agencia. En éste sentido, la seguridad de la información debe cumplir con tres características principales:

- Confidencialidad: es la propiedad que impide la divulgación de información a personas o sistemas no autorizados.
- Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- Autenticación: Es la propiedad que permite identificar el autor de la información o aquella que realiza modificaciones del contenido. [5]

C. *Protocolos de la Seguridad de la Información*

Los protocolos de seguridad son un conjunto de reglas que se aplican durante la transferencia de datos entre dispositivos para mantener la confidencialidad, integridad y autenticación de la información [5]. Se componen de:

- Cifrado de datos o archivos: Alteraciones de la información a través de programas compresores y encriptadores de datos informáticos
- Estructura y secuencia: Orden en el cual se agrupan los datos y control de tiempo de intercambio de información.
- Validación: Identificación técnica mediante el cual un proceso comprueba que el receptor de comunicación es quien se supone que es y no se trata de un impostor.

D. *Amenazas de los sistemas de información informáticos*

Los sistemas informáticos están constantemente bajo las siguientes amenazas:

- Programas maliciosos: virus, espías, troyanos, gusanos, phishing, spamming, entre otros.
- Siniestros: robos, incendio, humedad, entre otros, los cuales pueden provocar pérdida de información.
- Intrusos: piratas informáticos pueden acceder remotamente (si está conectado a una red) o físicamente a un sistema para provocar daños.
- Operadores: los propios operadores de un sistema pueden debilitar y ser amenaza a la seguridad de un sistema ya sea por falta de capacitación o de interés en el área, como por la venta de información con intereses económicos. [6].

E. *Importancia de la seguridad de la información*

La seguridad de la información es importante porque permite garantizar el correcto funcionamiento de las actividades dentro de la agencia, protege ante posibles fallos humanos, evita que usuarios internos puedan ser atacados por sistemas externos, previene la entrada de intrusos en los sistemas, impide que usuarios descontentos puedan causar daños importantes que lleguen a alterar o incluso a detener las actividades de la agencia y principalmente evita el filtrado o pérdida de información confidencial [7]. En consecuencia, para una correcta gestión en la seguridad de la información debe existir una planificación estratégica para enfrentar los riesgos, vulnerabilidades y amenazas que perturban a los sistemas de información de la ABAE durante su ciclo de actividad y durante el desarrollo de proyectos espaciales.

En el siguiente esquema (Figura 1) se muestran los elementos básicos de un sistema de gestión:

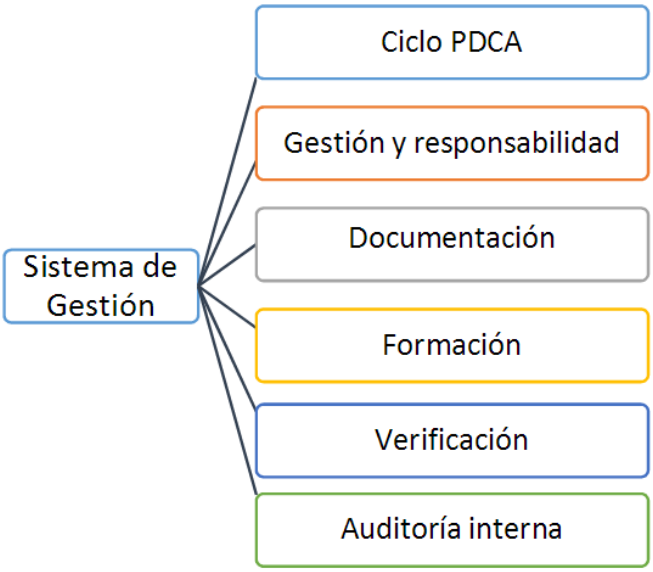

Figura 1: Estructura del Sistema de Gestión para la Seguridad de la Información.

III. Sistema de Gestión para la Seguridad de la Información

La mayoría de los problemas de seguridad de la información se deben a un conjunto de fallas en la implementación y desarrollo del proceso de seguridad de la información [8]. Para enfrentar estas carencias dentro de la agencia se debe crear e implementar un Sistema de Gestión para la Seguridad de la Información - SGSI (ISO/IEC 27001) y afrontar los siguientes tópicos:

- Crear las normativas (políticas, normas y procedimientos) para regir la organización de los recursos informáticos y su correcto uso (por ejemplo, el uso del correo electrónico institucional y de la información que por dicho medio se transfiere).
- Gestionar el control de acceso para las distintas clases de información, a través de niveles de usuarios, clasificación de áreas de acceso e inclusive clasificando la información por jerarquía (crítica, valiosa, sensible) con el objetivo de identificar qué usuario posee permisos para ejecutar determinada acción sobre una información.
- Crear la figura de "Administrador de la Información" para la gestión de la seguridad de la información y que ejerza

las responsabilidades como autoridad para la distribución de determinada información hacia los usuarios.
- Elaborar de planes de contingencia para el desarrollo de los procesos o políticas para la seguridad de la información.
- Crear y mantener las políticas de registros de acceso y modificaciones en los sistemas informáticos e inclusive en los procesos de creación y modificación de la información generada durante los proyectos que desarrolla la ABAE.
- Implementar las políticas para la creación de copias de seguridad de la información para salvaguardar los datos frente a situaciones catastróficas o pérdida de avances importantes en el desarrollo de los proyectos de la agencia. Por tal motivo, la creación de las copias de seguridad debe mantenerse permanentemente bajo actualización en caso de que se requiera una restauración.
- Crear la figura de "Administrador de proceso para Seguridad de la Información", responsable de la creación y actualización de los procesos de seguridad para el manejo de la información en los proyectos emergentes y en desarrollo.
- Gestionar los riesgos para el análisis de las amenazas y vulnerabilidades presentes en los sistemas de información de la ABAE y para mantener un control sobre posibles daños que pueden concurrir por efecto de la pérdida de información de carácter valiosa.
- Preparar planes de entrenamiento y concientización para las personas que laboran dentro de la agencia con la finalidad de notificarles las responsabilidades y actividades que pueden o no hacer con la información que crean, manejan o se distribuyen.

A. *Ventajas del SGSI*

El SGSI ofrecerá un método sistemático y bien estructurado para proteger la confidencialidad de la información, asegurará la integridad de datos de la agencia y mejorará la disponibilidad de los sistemas de tecnologías de la información, traduciéndose en las siguientes ventajas:
- Reducción de riesgos mediante una metodología de información estructurada que identifica y mitiga las amenazas.
- Resguardo de la información confidencial de amenazas como la piratería, la pérdida de datos, la violación de confidencialidad.
- Establecimiento de planes de contingencia para asegurar las operaciones continúas en caso de desastres naturales o causados por el hombre. B. Políticas para la seguridad de la información

B. *Políticas para la seguridad de la información*

La seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema, a través de la configuración de los mecanismos de autentificación y control que aseguran que sólo los usuarios de estos recursos posean los derechos que se les han otorgado [1].

Los mecanismos de seguridad se deben constituir de modo que no impidan que los usuarios desarrollen sus actividades y la información se maneje de forma segura. Por lo tanto las políticas de seguridad se deben implementar en función a:
- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la agencia, así como las posibles consecuencias por la pérdida de información
- Proporcionar una perspectiva general de las reglas y los procedimientos que se deben implementar para afrontar los riesgos identificados en las diferentes Direcciones/ Unidades o departamentos de la agencia.
- Controlar y detectar las vulnerabilidades del sistema de información y mantenerse informado acerca de los errores en las aplicaciones y en los materiales que se usan
- Identificar y analizar los factores de riesgo que atañen la seguridad de la a i información.
- Definir las acciones a realizar r y las personas a contactar en caso de detectar una amenaza. Implementar las reglas a seguir para el manejo de información de índole confidencial.
- Definir las políticas para el uso de la información, los recursos informáticos y los derechos de acceso de la información

La seguridad de la información de agencia depende de que los empleados (usuarios) aprendan tales reglas a través de sesiones de capacitación y concientización que permitan cubrir las siguientes áreas:

Los mecanismos de seguridad física y lógica implantados para cubrir las necesidades de la agencia, principalmente guardias de seguridad, vigilancia perimetral, controles de accesos, cifrado de la información, detectores de intrusos, antivirus, entre otros. --Los procedimientos para administrar las actualizaciones tanto de lasas aplicaciones como de la información que está en constante desarrollo. Las estrategias de creación n de copias de seguridad periódicas.

Los planes de recuperación desde la información luego de incidentes. Las actualizaciones de los sistemas de información documental.

El adiestramiento del persona en los temas de seguridad de la información (SI) y en el manejo de la información de manera segura.

La supervisión e implementación de mecanismos para proteger la información. Fundamentalmente se debe buscar el correcto y seguro uso de los sistemas informáticos en la agencia a través de los mecanismos de seguridad física y lógica dentro de las direcciones o unidades, con el objetivo de proteger la información. Entre los mecanismos de seguridad destacan los siguientes: Criptografía de paquetes de datos con información confidencial a nivel físico (HARWARE) como a nivel de programas (SOFTWARE).
- Firma digital.
- Autenticación.
- Control de acceso.
- Detección, registro e informe de eventos
- Control de redes informáticas
- Resguardo de la información digital a través de copias de seguridad en CD-ROM.

IV. Fundamentos de la Seguridad de la Información

La norma ISO/IEC 27001 considera como las tres principales características para que exista la seguridad de la información a:

la disponibilidad, la confidencialidad y la integridad. Estas características son fundamentales y deben estar presentes en todas las áreas de información donde se maneje información valiosa e inclusive aquellas que son de restringido acceso.

Los datos que se procesan electrónicamente se exponen a constantes amenazas y riesgos. Por consiguiente, aumentan las exigencias de seguridad cuanto a disponibilidad, confidencialidad e integridad de la información (ver Figura 2). Esto implica la protección de los sistemas informáticos y comunicación frente a las ofensivas crecientes, así como, la prevención de pérdidas por robo, los daños causados por acciones externas o comportamiento negligente del empleado de la agencia cuanto al trato de la información.

Figura 2: Bases para la seguridad de la información

Figura 3: Estructura de la información bajo el SGSI

El comportamiento consciente de los empleados en el ámbito de la seguridad de la información es un requisito fundamental para conseguir una protección integral de los datos. Por lo tanto, la implementación de un sistema integral de Gestión de Seguridad de la Información (SGSI) basado en la norma internacional ISO/IEC 27001 permite la identificación sistemática y el análisis de riesgo, que surge con el uso de la información hasta la implementación y el mantenimiento de los mecanismo adecuados de vigilancia y control [9].

La seguridad de la información consta de requisitos formales y expectativas, estos abarcan toda la agencia y es más que simplemente almacenar y procesar datos, es también integridad, disponibilidad y confiabilidad para que exista la credibilidad, responsabilidad, constancia y confianza en la información (ver Figura 3).

A. *Implementación del SGSI*

El SGSI consta de todos los elementos necesarios para planificar, definir, implantar, verificar y supervisar las medidas de seguridad necesarias para cumplir los requerimientos de seguridad que la ABAE requiere en sus proyectos espaciales.

El Sistema de Gestión de Seguridad del Información es un proceso continuo, basado en el modelo PDCA (Plan-Do-Check-Act) (Ver Figura 4). Este sistema permite identificar y analizar los posibles riesgos, las necesidades de actuación y las medidas necesarias para supervisar y optimizar el trato de la información continuamente.

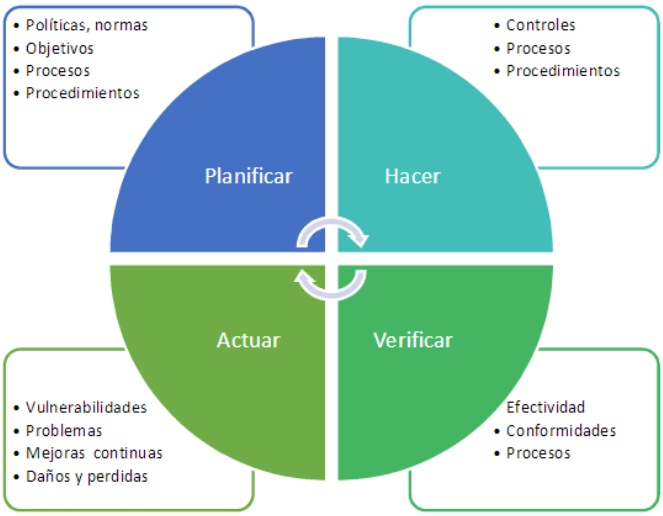

Figura 4: Modelo Plan-Do- Check-Act

Planificar: para establecer las políticas, objetivos, normas, procesos, procedimientos necesarios para gestionar los riesgos y mejorar la seguridad de la información, de acuerdo a las necesidades y requerimientos de la ABAE.

Hacer: para implantar y operar las políticas, procesos, procedimientos y controles definidos.

Verificar: para evaluar la eficacia y eficiencia de las políticas, procesos, procedimientos y controles para alcanzar los objetivos de seguridad de la información definidos e identificar aquellas no conformidades con la planificación realizada.

Actuar: para definir las medidas preventivas y correctivas destinadas a solucionar las no conformidades detectadas, a mejorar el cumplimiento de los requerimientos de seguridad de la información definidos y adaptar el sistema a los cambios internos y externos relevantes [2]

B. *Factores para la Implementación del SGSI*

- Las políticas, medidas y objetivos de la seguridad de la información deben estar orientados a los objetivo de la ABAE.
- El modelo PDCA debe estar estructurado en concordancia con las políticas de seguridad de la institución y en concordancia con los de la nación.
- Las direcciones de la agencia deben apoyar aprobar el SGSI para a implementarlo en las unidades que la conformen.
- Debe existe una buena a comprensión de valoración y gestión de riesgos para poder enfrentarlos con la solución más favorable para la agencia
- Planificación para difundir las políticas de seguridad de la información a todos los niveles y empleados
- Los costos y presupuestos deben cubrir todas las actividades de gestión de seguridad de la información
- Los procesos deben ser eficaces frente a incidentes de seguridad de la información
- El sistema de indicador debe garantizar la eficiencia y mejoras del SGSI

Estos factores definidos en la institución permitirán la implementación del SGSI basado en la ISO/IEC 27001, el cual incrementara lo niveles de confianza en el manejo de la información y datos desarrollado en los proyectos de índole nacional e internacional, restringiendo así el uso de la información dependiendo de clasificación o importancia, para que sea accedida por las personas autorizadas y para que las partes externas interesadas se les exija cumplir con los requisitos implementados por la agencia para tener acceso a la [9]. Si además se busca que el SGSI también sea auditado y certificado por un especialista externo se logrará un sello de calidad de la información que permitirá avanzar de manera segura durante el desarrollo de proyectos espaciales en la ABAE.

C. *Gestión de Riesgo de la Información.*

La gestión de riesgo consta de elementos fundamentales: la identificación, la valoración y la implementación de controles de riesgos.

Los controles afectan directamente los siguientes aspectos en la agencia:

- Seguridad física y del entorno de trabajo
- Seguridad ligada a los RRHH
- Seguridad de comunicaciones y operaciones
- Control de accesos a las instalaciones
- Seguridad en la fase de diseño y desarrollo de proyectos
- Gestión de incidentes en la Seguridad de la Información durante los procedimientos de emergencia
- Cumplimiento de las actividades.

Los riesgos no pueden ser totalmente eliminados, pero sí pueden ser continuamente reducidos si se implantan medidas coherentes que ataquen las vulnerabilidades de los sistemas que almacenan la información, por ello, el análisis de riesgos. Por otra parte, la solución que se implemente tiene que basarse en objetivos realistas fundamentados a través de los estudios de costo/beneficio. Por lo tanto, las medidas de seguridad a implementar tendrán que ser consecuentes con los análisis realizados.

V. MANEJO DE LA INFORMACIÓN CONFIDENCIAL

La información confidencial de la agencia comprende desde información técnica, secretos comerciales hasta tratados internacionales que no son difundidos para su protección legal, por tal motivo debe existir un trato especial de resguardo frente a terceros ajenos a la agencia e incluso internamente a través de la implementación de acuerdos de confidencialidad, los cuales permiten proteger los datos proporcionados y que permiten dejar en claro el uso al cual está destinada la información [10].

La confidencialidad de la información se puede implementar a través de códigos especiales durante la identificación de documentos o datos informáticos, esto con la finalidad de que sólo el personal autorizado pueda utilizar eficientemente dicha información. Por otro lado, el número de personas con acceso a dicha información debe ser limitado, es decir sólo aquellas personas involucradas directamente en áreas técnicas o gerenciales del proyecto (nacionales o internacionales) deben manipular los datos de índole confidencial, y se pueden utilizar contraseñas personales para poder acceder a los datos, las cuales deben registrar quiénes accedieron a la información.

Por otro lado, los registros de papel (documentos, manuales, procedimientos que posean información confidencial) se deben resguardar en un lugar cerrado y protegido con un sistema de seguridad mientras no se estén utilizando, y cuando el material haya cumplido su objetivo (vida útil) deberá ser destruido con la debida autorización de la dirección a la que pertenece y en algunos casos con la autorización de la presidencia de la agencia.

Los mecanismos de cifrado y ocultación de la información permite garantizar la confidencialidad a través del uso de la llaves asimétricas durante un determinado tiempo, pero en resumen no existe mecanismo totalmente seguro, por tal motivo, lo recomendable es el uso combinado de técnicas para mejorar la confiabilidad de los datos confidenciales.

A. *Pasos para la Protección de los Documentos Confidenciales*

- Identificar la información sensible a través de la clasificación de los documentos, donde la información confidencial esté disponible de forma restringida a la empresa y no está disponible públicamente.
- Asegurar que los empleados de la agencia y las partes involucradas en los proyectos tenga conciencia de la gestión de información confidencial a través de planes de capacitación o culturización para el manejo y protección de la misma.
- Utilizar Acuerdos de Confidencialidad (NDA; Non-Disclosure-Agreements) cuando se vaya a compartir información importante con terceros.
- Proteger la información confidencial y limitar el acceso a la misma de tal manera que sólo el personal involucrado en el área o proyecto tenga acceso.
- Identificar y monitorear quién tiene acceso a la información confidencial y el uso dado a la misma por los involucrados [11].
- Mantener la documentación digital bajo sistemas de encriptación y contraseñas con cambios periódicos de acuerdo a las políticas de seguridad [12].

- Ejecutar acciones de respaldo de la información confidencial en dispositivos con alta credibilidad en seguridad y resguardado por los directivos de la agencia.
- Evitar el uso de los servicios de nube, correos electrónicos, dispositivos móviles USB para proteger la información confidencial.
- Destrucción de la información confidencial con accesibilidad física al finalizar su vida útil.

B. *Acuerdos Confidenciales*

Los acuerdos de confidencialidad o cláusulas de confidencialidad son una manifestación de carácter legal en donde se detalla la obligación de guardar y no revelar a terceros información que la agencia desea que se mantenga confidencial. Los principales elementos que conforman el documento son los siguientes:

- Las obligaciones del usuario de la información.
- El uso destino de la información y la factibilidad de reproducción.
- Las sanciones o multas en se incurrirá en caso de incumplimiento.
- Las excepciones a la confidencialidad
- Las limitaciones de la responsabilidad del usuario

En el ámbito interno de la agencia, resulta igualmente indispensable que se identifique la información confidencial que se pretende proteger y que se les comunique a los trabajadores que tengan acceso a la misma para su trato adecuado en concordancia con las políticas del SGSI. Además es conveniente revisar periódicamente qué empleados tienen acceso a dicha información y aplicar restricciones para acceder a ésta e inclusive renovar por medio de un documento legal las cláusulas de confidencialidad [10].

C. *Funciones del Acuerdo de Confidencialidad*

La función principal del acuerdo de confidencialidad es la de proteger la información técnica o comercial que no se desea divulgar a terceros, esto se logra a través de un compromiso legal para no divulgar la información recibida entre las partes involucradas.

Si la información se revela a otra empresa o difunde abiertamente, la parte perjudicada tiene motivos para reclamar un incumplimiento del acuerdo de confidencialidad (contrato o clausulas) y además, puede reclamar daños y perjuicios cautelares y económicos de índole legal. En otras palabras el acuerdo de confidencialidad se crea principalmente para:

- Prevenir la pérdida de valiosos derechos de propiedad intelectual.
- Definir la información que puede y no puede ser divulgada a través de la clasificación de la información (confidencial o reservada) [4].
- Limitar el uso específico de la información confidencial.
- Establecer un período de tiempo durante el cual se realizarán las revelaciones o intercambio de información entre las partes involucradas y el período durante el cual la confidencialidad de la información se ha de mantener.

VI. DESTRUCCIÓN DE LA INFORMACIÓN CONFIDENCIAL

El ciclo de vida de la información consta de tres etapas: generación, conservación y destrucción de la información confidencial (IC). La importancia de la última etapa radica en asegurar que la confidencialidad que ha acompañado a la información durante las fases previas de su ciclo de vida se mantenga hasta que se decida que ya no es útil y sea destruida para evitar que terminen siendo de dominio público.

Debido a la importancia de esta etapa, la agencia debe crear y poseer un procedimiento claro dentro de sus políticas para la protección de la información confidencial una vez esta haya cumplido su vida útil, para esto la información debe cumplir con las siguientes características:

- Ser secreta, es decir que no sea generalmente conocida ni fácilmente accesible.
- Tener un valor comercial por ser secreta.
- Haber sido objeto de medidas razonables para mantenerla secreta [13].

Por ende la agencia debe garantizar la seguridad y la confidencialidad de la información a lo largo del ciclo de vida a través de los protocolos de creación, gestión, archivamiento y destrucción para evitar poner en riesgo a la agencia por robo, uso indebido, divulgación e inclusive sufrir sanciones legales por el incumplimiento de la custodia de dicha información. Entre los elementos que poseen IC y que se deben destruir se presentan los siguientes:

- Documentación en papel.
- Documentación en fichas plásticas.
- Formatos digitales (CD, HDD, DVD, Blue Ray, cintas magnéticas, unidades Flash USB, entre otros).
- Documentación contenida en los teléfonos, PDA, correos electrónicos, nube, entre otros.

A. *Proceso de Destrucción de la IC*

El proceso de destrucción consta de las siguientes etapas:

- Etapa de Solicitud: Se solicita el servicio de destrucción de forma que se identifique la información a destruir.
- Etapa de recopilación: Se recolectan los soportes, datos, dispositivos, elementos y se informa al usuario que no se podrá continuar con el uso de la misma ni recuperar la información.
- Etapa de transporte y almacenamiento: La IC es transportada y almacenada en un mismo lugar para su destrucción (Se requiere de medidas de seguridad física y custodia de zona).
- Etapa de destrucción: Se procede a la destrucción física de la IC y de los dispositivos que la contengan.
- Etapa de confirmación: verificación del proceso de destrucción de forma segura y notificación que la actividad se ha ejecutado satisfactoriamente [13].

B. *Normas y Procedimientos Generales para la Destrucción de la IC*

La ABAE debe crear la normativa y los procedimientos para el proceso de destrucción de la IC según las políticas para el manejo de la información a través del SGSI. Los elementos más importantes que deben estar contenidos en la normativa son los siguientes:

- Clasificación de la información que existe en la agencia.
- Identificar todos los usuarios de la IC.
- Especificación del trato de la información una vez deja de ser útil para la agencia.

- Especificación de los procedimientos para realizar la destrucción o borrado de la información según el soporte en el que se encuentre almacenada.

Por lo tanto, la normativa debe asegurar que los dispositivos electrónicos serán tratados adecuadamente para lograr un borrado seguro y pasos para la confirmación y la desaparición real de la información. En caso de no poder hacer un borrado, por ejemplo, cuando el soporte utilizado es el papel, teléfonos móviles, entre otros; se procederá a la destrucción física del elemento en cuestión, y esta deberá ser llevada a cabo "in-situ" para evitar problemas durante el transporte y la custodia de la misma [13].

VII. Auditoría del Sistema de Gestión de Seguridad de los Sistemas de Información

La auditoría de los sistemas de información (SI) comprende el análisis y gestión de sistemas para identificar, enumerar y clasificar las vulnerabilidades que acarrean riesgo en la perdida de la información de la agencia ya sean accidentales o intencionales [14]. Esta actividad se realiza con la finalidad de certificar y poner a prueba el sistema de gestión para seguridad de la información en todos sus niveles.

A. *Fases de la auditoría*

- Verificación de los controles de riesgos.
- Enumeración de estaciones de trabajo, puertos, redes, topologías y protocolos implementados de la agencia.
- Verificación del cumplimiento de las políticas, medidas y controles implementados para el resguardo de la información.
- Identificación de los sistemas operativos instalados, puerto habilitado y dispositivos de almacenamiento de la información.
- Análisis de servicios y aplicaciones.
- Detección, comprobación y evaluación de vulnerabilidades.
- Medidas específicas de corrección.
- Recomendaciones sobre implantación de medidas preventivas [14].

VIII. Conclusiones

En la ABAE aún existen vulnerabilidades en los sistemas que manejan información que conllevan a la perdida de información valiosa, pero con la implementación correcta del SGSI se podrán ejecutar los controles correctos para minimizar los riesgos de perder información confidencial y aumentar los niveles de seguridad para el trato de la información que la agencia maneje durante sus proyectos nacionales e internacionales.

Con la implementación del SGSI se podrá aplicar el modelo de PDCA estructurado y ajustado a las necesidades de la agencia, en donde se podrán atacar las vulnerabilidades y problemas informáticos que surgen debido a la existencia de la información confidencial de los proyectos en el área de tecnología espacial como es el caso de diseño, ensamblaje e integración de satélites. Por otro lado, preparar principalmente a los empleados y usuarios de la información a través de planes de capacitación para el correcto uso de la información interna de la agencia y de la notificación de la existencia de información confidencial a través de los acuerdos de confidencialidad para la no divulgación de la información a terceros o hacerla pública sin autorización. Y además creando las normativas y procedimientos para la etapa de destrucción de la información la cual servirá como un mecanismo adicional que permitirá proteger los bienes intelectuales de la agencia, cumplir con las políticas para control y uso de la información y lograr un alto nivel en el manejo de la seguridad de la información en los proyectos satelitales.

Referencias

[1] [1] CCM_High-Tech, «CCM.net,» 03 2016. [En línea]. Available: http://es.ccm.net/contents/622-introduccion-a-la-seguridad- informatica. [Último acceso: Mayo 2016].

[2] [2] Juan_M, «ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN,» 2009.

[3] [3] Asamblea Nacional, «LEY DE INFOGOBIERNO,» 2013.

[4] [4] Llamazares_O, «Globalnegotiator.com,» [En línea]. Available: http://www.globalnegotiator.com/blog/que-es-un-contrato-de- confidencialidad/. [Último acceso: 04 2016].

[5] [5] Fundación_Wikimedia_Inc., «Wikipedia.org,» [En línea]. Available: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B 3n. [Último acceso: 04 2016]. [6] Nelsy_L, «Conociendo Venezuela,» [En línea]. Available: http://conociendovenezuelaconnelsy.blogspot.com/p/seguridad- informatica_31.html. [Último acceso: 04 2016].

[6] [7] Llorente_M, «DSA_Research,» 05 2008. [En línea]. Available: http://dsa-research.org/lib/exe/fetch.php?media=people:llorente:seguridad _en_las_tecnologias_de_la_informacion.pdf.pdf. [Último acceso: 04 2016].

[7] [8] Pores_M, «Informaticahoy.com,» [En línea]. Available: http://www.informatica-hoy.com.ar/seguridad-informatica/Fallos- de-Seguridad-en-la-Informacion.php. [Último acceso: 04 2016].

[8] [9] ISO, «TUV_sud.es,» [En línea]. Available: http://www.tuv-sud.es/uploads/images/1350635458019372390409/pdf2-0039- iso-iec-27001-es-260412.pdf. [Último acceso: 04 2016].

[9] [10] Erendira_Ramirez, «CNN_expansion,» 06 2015. [En línea]. Available: http://blogs.cnnexpansion.com/consultorio-fiscal-y-juridico/2015/07/07/resguarda-la-informacion-confidencial-de- tu-empresa/. [Último acceso: 04 2016].

[10] [11] Sealpath, «Sealpath.com,» [En línea]. Available: http://www.sealpath.com/es/nosotros/blog/item/179-5-pasos- para-proteger-mejor-tus-documentos-confidenciales. [Último acceso: 04 2016].

[11] [12] Guánchez_V, «Emprendovenezuela.net,» 09 2012. [En línea]. Available: http://www.emprendovenezuela.net/2012/09/5- pasos-para-una-mayor- seguridad.html. [Último acceso: 04 2016].

[12] [13] C. C. Gema_L, «gpd.sip.ucm.es,» [En línea]. Available: http://gpd.sip.ucm.es/sonia/docencia/master/Trabajos%20Alumnos/Destruccion%20segura%20de%20datos/DestruccionSegur aDatos.pdf. [Último acceso: 04 2016].

[13] [14] Fundación_Wikimedia_Inc., «Wikipedia.org,» [En línea]. Available: https://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_d e_sistemas_de_informaci%C3%B3n. [Último acceso: 04 2016].

Nacido en Venezuela, Estado Bolívar en 1985. Egresado UNEFA-2007 como Ingeniero Electrónico, empleado ABAE desde 8-2014. Desde 2015 asignado en la Unida de Desarrollo de Productos y Procesos perteneciente a la Dirección de Investigación y Desarrollo. Actualmente las Funciones delegada están dirigidas al desarrollo del Centro de Investigación y Desarrollo Espacial (CIDE) y el Satélite Sucre (VRSS-2).