Manejo en la Seguridad de la Información
Management of Information Security

Arturo Rojas, Ingeniero en Diseño, Integración y Pruebas Satelitales, *ABAE*

***Resumen*—Se abarcan diferentes estrategias para salvaguardar la seguridad de la información confidencial. Se hace mención a los lineamientos fundamentales implementados por empresas en el área de la tecnología satelital, para proteger su activo más importante, la información. También se incluye cuales parámetros deben tomarse en cuenta cuando la información satelital confidencial es compartida entre empresas, esto en el contexto de desarrollo de proyectos conjuntos. Igualmente se definen algunos términos como portadores, estos son CD, memorias, entre otros y se mencionan algunas políticas correctivas aplicadas a empleados cuando ellos hacen uso incorrecto en el manejo de la información. También se incluye procedimientos sencillos como el registro de personas en el proceso de almacenamiento de archivos. Se hace hincapié en la importancia del envió de información por internet, haciendo una clara diferencia entre redes internas y redes externas.**

***Palabras claves* — Confidencialidad, portadores, redes, reuniones.**

***Abstract*—It is included some strategies in order to save the security of the confidential information. It is mention the main fundamental policies implemented by companies on the satellite technological area, in order to protect its most valuable active, the information. Also, in this document is included which parameters should be taken account when the satellite confidential information is shared among companies, this in the context of development of projects as joint-team. Additionally, some terms are defined such as carriers, for example CDs memories and others; it is mentioned some corrective policies applied to employees when they make use of non-right manage of information. Also, this document includes procedures such as registers of people in the process of storage of files. Relevant comments are made in order to demonstrate the importance concerning to delivery of information by internet, making a clear difference between open networks and point to point networks.**

***Index terms*—Carriers, confidentiality, meetings, nets.**

I. Introducción

El objetivo de este documento es hacer un primer acercamiento en las estrategias empleadas por distintas instituciones respecto al manejo de la información confidencial. Se ha incluido normas procedentes de la experiencia en el desarrollo del satélite VRSS-2. En el desarrollo de este documento se hace notar que la información es un activo que tiene valor para una empresa y consecuentemente requiere ser protegida adecuadamente.

10 de Julio de 2017. El autor trabaja en el Centro de Investigación y Desarrollo Espacial de la ABAE (arojas@abae.gob.ve).

II. Gerencia en la seguridad de la información

En el proceso de desarrollo de proyectos de envergadura, tales como el desarrollo de proyectos satelitales, se hace necesaria la implementación de conocimientos, técnicas, procedimientos que son específicos y que permiten construir naves espaciales que tienen un impacto relevante en la sociedad. Por ejemplo, estas naves espaciales son capaces de tomar registros fotográficos de zonas específicas del planeta, transmitir datos sensibles tales como comunicaciones gubernamental es internas, resultados electorales, comunicaciones militares, internet, televisión, entre otros. Es por esto que las grandes compañías que desarrollan naves espaciales son precavidas para liberar información referente al proceso de desarrollo de satélites. Para manejar este tipo de información, usualmente se establece la figura del Gerente de la Seguridad de la Información para asegurar que el personal bajo su mando reciba la educación necesaria en seguridad para asegurar la apropiada ejecución de sus responsabilidades, como se muestra en la referencia [1].

Es importante notar que el contenido de la información tiene diferentes niveles de valoración. Por ejemplo, el impacto que puede tener un procedimiento para la manufactura de un amplificador pasa banda es diferente al de un procedimiento el cual describa el proceso de obtención de plutonio enriquecido. Es por esto que alrededor del mundo, se establecen niveles de clasificación de la información, como se muestra en la referencia [2], pudiéndose destacarse las siguientes:

1) Altamente secreto (top secret): es el nivel más alto de clasificación de la información. Si la información que esta almacenada con esta etiqueta es liberada, se pueden ocasionar daños excepcionales a la seguridad de empresas o/y naciones.
2) Secreto (secret): es un nivel intermedio en la clasificación de la información. Si la información es liberada implica que la revelación de información no autorizada pudiera razonablemente causar serios daños a la seguridad de la empresa o/y naciones.
3) Confidencial (confidential): es el nivel más bajo en la clasificación de la información. Si la información que esta almacenada con esta etiqueta es almacenada, implica que la revelación no autorizada de información pudiera razonablemente causar un daño a la empresa o/y naciones.

La información que tiene una etiqueta de confidencialidad (top secret, secret, confidential) debe cumplir con unos

criterios de almacenamiento y de destrucción, cuando se requiera. El personal relevante que tiene acceso a la información confidencial tiene el deber de almacenar la información clasificada, y destruirla cuando corresponda. Se pueden mencionar los siguientes lineamientos para el almacenamiento de información confidencial, obtenidos de la experiencia de desarrollo del satélite sucre:

1) El personal de seguridad se asegurara que todas las informaciones clasificadas estén almacenadas de una manera que detecte o disuada el acceso a personas no autorizadas.
2) Armas, dinero, joyas, metales preciosos o narcóticos no serán almacenados en los contenedores de seguridad usados para almacenar información clasificada. Los contendores que contienen información clasificada tienen a no ser revisados en aduanas, alcabalas, entre otros. Por lo que este tipo de contenedores es considerado para el tráfico de elementos diferentes a los que inicialmente están destinados.
3) No habrá marcas externas que revelen el nivel de clasificación de la información que está siendo almacenada en un contenedor específico de seguridad. De existir marcas externas, se le estaría dando referencias para la ubicación de la información a los espías y personal no autorizado.
4) Información clasificada cuya vigilancia no está bajo el personal de control u observación claramente apropiado, será guardada o almacenada en un contenedor de seguridad sellado aprobado por instancias superiores.
5) La localización del contenedor será sujeta a continua protección por el personal adecuado.
6) Un sistema de detección de intrusos, con el personal alerta a la alarma dentro de un periodo de tiempo adecuado luego de la activación de la alarma.

Adicionalmente, el control de documentos permite definir las acciones que conduzcan a un manejo adecuado de datos para preservar la confidencialidad. A continuación se mencionan lineamientos relevantes para el control de documentos, como se muestra en la referencia [3]:

1) Certificar que los documentos se mantengan legibles y fácilmente identificables.
2) Certificar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso.
3) Certificar que se identifiquen los cambios y estatus de la revisión actual de los documentos.
4) Aprobar la idoneidad de los documentos antes de su emisión.
5) Revisar y actualizar los documentos conforme sea necesario y re-aprobar los documentos.
6) Certificar que se identifiquen los documentos de origen externo.
7) Asegurar que se controle la distribución de documentos.
8) Evitar el uso indebido de documentos obsoletos.
9) Aplicarles una identificación adecuada si se van a retener por algún propósito.
10) Asegurarse que los documentos estén disponibles para el personal que los necesite previa autorización, y sean transferidos, almacenados y finalmente eliminados en concordancia con los procedimientos aplicables para su clasificación.

Aunque las empresas y las naciones tienden a salvaguardar la información que puede tener un impacto en el desarrollo de proyectos, sociedades, entre otros, existen limitaciones para el establecimiento de la clasificación de la confidencialidad de la información, se mencionan a continuación las más relevantes, como se muestra en la referencia [2]:

1) Usar clasificación para esconder violaciones a la ley, ineficiencias o errores administrativos.
2) Clasificar información para prevenir humillaciones a una persona, organización o agencias.
3) Clasificar información para restringir a la competencia.
4) Clasificar información para prevenir o retrasar la liberación de información que no requiere protección en el interés de la seguridad nacional.
5) Clasificar información de investigaciones científicas básicas no claramente relacionadas a la seguridad nacional.
6) Clasificar un producto de una investigación no-gubernamental que no incorpora o revela información clasificada para la cual el productor o desarrollador se le fue dado acceso prioritario.
7) Clasificar, o usar una base para la clasificación, para hacer referencias documentos, cuando la cita no revela en si misma información clasificada.

III. ESTRATEGIAS DE CONFIDENCIALIDAD PARA PROYECTOS INTERNACIONALES

En el marco de desarrollo del programa satelital VRSS-2, se emplearon una serie de acciones para preservar la confidencialidad de la tecnología, procesos, datos que se estaban manejando en el proceso de desarrollo del satélite. A continuación se mencionan algunos ítems relevantes que fueron tomados en cuenta en las actividades diarias desarrolladas en el programa espacial, como se muestra en la referencia [3]:

1) No traer cualquier artículo o pertenencia que no esté permitida por la empresa dentro del área de oficina o facilidad.
2) No relacionarse en negocios o actividades comerciales que interrumpan el trabajo pre-asignado.
3) No acceder indebidamente a los ítems de confidencialidad de la empresa.
4) No usar, a menos que tenga a priori una autorización, cualquier material provisto por la empresa para cualquier propósito que este fuera del contrato.
5) No copiar, transcribir y fotocopiar los libros, material de entrenamiento, parámetros técnicos, programas, planos, manuales, documentos literatura, registros, software, otras informaciones y materiales obtenidos desde la empresa o producida por la empresa que no ha sido publicada en el dominio público.

6) No proveer o revisar cualquiera de los materiales relacionados arriba mencionados a cualquier tercera parte, directamente o indirectamente, sin el consentimiento a priori de la empresa.
7) Cualquier reporte de prensa, declaración a los medios, ubicaciones técnicas o reporte a terceras partes (por ejemplo aseguradoras, plan de trabajo del programa, entre otros) que se refieren al uso de procedimientos técnicos empleados en el programa (satelital), provisto por la empresa será aprobado por la empresa a priori de la liberación. Los documentos y reportes no serán enviados por cualquier sistema de comunicación no-encriptado.

IV. Lineamientos generales de interacción entre empresas en el manejo de información.

El intercambio de información en proyectos de cooperación internacional entre empresas impone el seguimiento de algunas normativas que deben ser tomadas en cuenta. Todas las actividades relacionadas a la implementación del contrato están restringidas por el contratista y todas las restricciones de seguridad del país a la cual se trabaja. Si se rompe el acuerdo arriba mencionado, la empresa está autorizada a terminar el acceso a las instalaciones de la empresa y finalizar el trabajo pre-asignado por la empresa. A continuación se muestran algunos ítems relevantes en lo que respecta al manejo de la información entre empresas procedentes de diferentes países, en este caso se mencionan los lineamientos más relevantes empleados en la cooperación Venezuela-China en el área espacial, como se muestra en la referencia [3]:

1) Capacidades en seguridad de Venezuela: es de suponer que es importante para el país con el cual se está interactuando este punto, ya que información clasificada de ese país es provista.
2) Manejo de personal para salvaguardar los secretos.
3) Cuentas personales son tomadas como secretas: esta política se puede evidenciar en las actividades de interacción entre el personal venezolano y el personal chino, ya que el personal chino utiliza cuentas de correo no oficiales para comunicarse con el personal venezolano.
4) La cooperación entre China y Venezuela es considerada un secreto de negocios, por lo tanto no está permitido dar a conocer esta cooperación.
5) Los secretos involucran el proceso de manufactura de máquinas.
6) Se debe tener cuidado con los espías.
7) ¿Cuál es la influencia y el contenido de páginas como Wikipedia?
8) Tomando en cuenta el escenario geopolítico mundial, los secretos pueden afectar a los países del medio oriente.
9) El manejo del personal que está envuelto en secretos es un punto a considerar.
10) La gerencia de los secretos envuelven el manejo del internet.
11) El manejo de los secretos envuelven portadores, es decir: documentos, USB, discos duros, que contienen información clasificada. A esto se le denomina objetos secretos.

V. Secretos envueltos en portadores

Lo primero que hay que plantearse es si el contenido de los portadores es secreto. Entonces se debe plantear cómo se determina si una información es un secreto. Esto se hace colocando una etiqueta a los secretos. Esta etiqueta provee información acerca del nivel de confidencialidad de dicha información. Luego de determinar el nivel de confidencialidad se debe plantear como usar esta confidencialidad establecida, lo cual implica establecer quien puede manejar la información de interés. Establecida esta estrategia, para cualquier persona que quiera archivar una información, necesita registrar su nombre para entonces el archivo ser codificado.

Es importante mencionar que los espías están interesados en coleccionar portadores de información. Por lo tanto para prevenir esto, los archivos se pueden manejar de dos formas, como se muestra en la referencia [2]:

1) Los archivos pudieran ser ajustados tal que pudieran mantener los procedimientos confidenciales bajo resguardo.
2) Los archivos se pueden destruir. Para hacer esto se necesitan de dos personas. En el caso de documentos, éstos se deben destruir totalmente quemándolos. Para los USB, discos duros, CD y otros se debe proceder a destruirlos físicamente totalmente.

VI. Reuniones e internet

Para comunicarse con los clientes, para hacer reuniones, entre otros, la exposición de secretos al público es evidente, por lo tanto se tiene que evitar hacer pública la información concerniente a la tecnología espacial. En este tipo de reuniones algunos ingenieros pueden filtrar accidentalmente información y esta información pudiera ser impresa. También hay que tener en cuenta que internet no es una muy buena manera de transmitir información. Los siguientes puntos deben ser considerados, como se muestra en la referencia [3]:

1) Los virus informáticos pueden robar información confidencial. Los virus son muy peligroso porque buscan automáticamente información en computadoras, teléfonos celulares, y cualquier artefacto que pueda tener acceso a internet o redes inalámbricas.
2) En las reuniones se discute y se intercambia información confidencial.
3) Si hay una reunión, se debe preguntar quién tiende a esa reunión.
4) Antes de las reuniones se deben identificar el ID de las personas.
5) Después de dejar el salón de reuniones, se debe asegurar que no existan documentos, portadores u algún otro tipo de ítem que contenga información confidencial que fue discutida en la reunión.
6) En cualquier reunión donde se discuta información confidencial, los teléfonos celulares no deben ser permitidos.
7) Los micrófonos no son permitidos.
8) Después de las reuniones, los portadores de información confidencial deben ser colectados.

9) Los dispositivos que envuelven secretos, tales como copiadoras, impresoras, entre otros, deben pasar el examen de seguridad.
10) Hay que tomar en cuenta que los dispositivos pueden tener programas que pudieran almacenar información sensible sin la autorización del usuario.
11) No es seguro conectar una computadora a internet con información confidencial. No es seguro conectar computadoras a redes abiertas.
12) Los dispositivos tales como USB, o cualquier tipo de hardware que almacene información confidencial deben ser registrados.
13) En este caso, los dispositivos que no estén registrados, no deben ser usados.
14) No está permitido conectar estos dispositivos registrados al internet.
15) Debe establecerse claramente la diferencia entre una red interna y las redes externas.

Para evitar errores, se debe establecer una regulación que es un proceso de mejoramiento de cada quien en el conocimiento de cómo proteger secretos. Esto es educación. A la par de que las personas involucradas deben tener la habilidad para proteger la información confidencial. Si se comenten errores en el manejo de la información confidencial por parte del personal involucrado, se deben aplicar sanciones al personal que cometió el error. Fundamentalmente existen dos tipos de sanciones en concordancia al tipo de error cometido:

1) Para errores pequeños o que tienen un impacto menor: el personal involucrado debe recibir un entrenamiento adicional concerniente al manejo de la información confidencial.
2) Para errores que tienen un impacto excepcional para la empresa: suspensión o despido.

VII. Acciones para proteger la información confidencial

A continuación se mencionan las acciones más relevantes para proteger la información, como se muestra en la referencia [3]:

1) Copiar la información a CD.
2) No usar redes inalámbricas. Ésta es una red abierta.
3) No conectar laptops a redes externas.
4) Solo usar fotocopiadoras autorizadas.
5) El teléfono es una computadora portable, por lo tanto no es confiable. Algunos teléfonos pueden escuchar. También falsas estaciones de celulares pueden ser usadas para espiar.
6) Aplicaciones de comunicaciones, tales como wechat son peligrosos porque se puede enviar información confidencial sin un control adecuado.
7) Es prohibido tomar fotos, fotocopiar, escanear documentos confidenciales con celulares u otros dispositivos de comunicación.
8) En cualquier momento se debe prestar atención a la protección de la información.
9) El personal debe tener la capacidad de percibir si dentro de un grupo de personas existe un espía.
10) Las puertas de acceso a los salones de reuniones deben tener un sistema de identificación del personal que accede.
11) Los documentos de diseño de satélites, procedimientos de pruebas, procesos de integración y ensamblaje satelital, planos entre otros no pueden ser enviados por una red de computadoras abiertas.
12) Crear una red interna para el intercambio de la información.
13) La información confidencial debe ser encriptada cuando es colocada en portadores y para procesos de almacenamiento.
14) Enviar documentos físicos por medio de servicios de envío confiables. Se deben establecer departamento de envíos internos no comerciales de la institución para asegurar la confidencialidad.
15) Las claves personales deben ser distintas a las claves del trabajo.

VIII. Ciber-seguridad de la información

La transmisión, almacenamiento y generación de datos entre computadoras hacen que éstas sean objetos de interés de espías y elementos interesando en recabar información. Con el fin de prevenir esto, las empresas establecen estrategias para protegerse de ciber-ataques. Fundamentalmente se toman de referencia los siguientes lineamientos para el establecimiento de la ciber-seguridad:

1) Desarrollar un entendimiento organizacional para manejar ciber-riesgos para los datos de los sistemas.
2) Desarrollar e implementar estrategias para salvaguardar los servicios críticos.
3) Desarrollar e implementar las actividades apropiadas para tomar las acciones tomando en cuenta un evento de ciber-ataque detectado.
4) Desarrollar e implementar las actividades apropiadas para tomar las acciones, teniendo presente un evento de ciber-ataque detectado.
5) Desarrollar e implementar las actividades apropiadas para mantener los planes para recuperar y restaurar cualquier capacidad o servicio dañado por un evento cibernético.

IX. Ejemplo de referencia en el manejo de información confidencial

Un ejemplo en las formas de cómo se maneja la información sensible es el de las fotografías del satélite en el proceso de desarrollo, como se muestra en la referencia [3]. En el proceso de ensamblaje e integración de satélites, se deben realizar registros fotográficos del satélite. Por cuestiones de seguridad, no se puede realizar un registro fotográfico del satélite a menos que sea especificado o en los documentos donde se describe la implementación del ensamblaje e integración del satélite o sea autorizado por la PMO (Program Management Office).

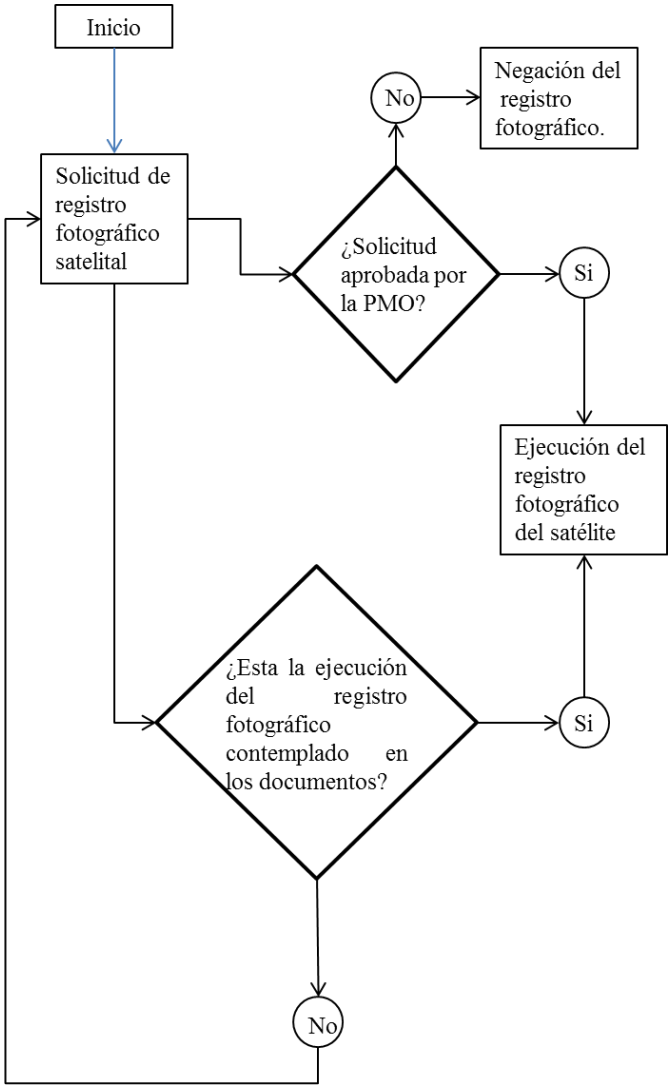

Fig. 1. Diagrama de flujo en la ejecución del registro fotográfico de satélites con fines técnicos.

Una vez autorizado el registro fotográfico del satélite en una etapa de desarrollo determinada, se establece quien debe hacer el registro fotográfico. En el caso satelital, solo el inspector de ensamblaje e integración puede tomar las fotografías. Adicionalmente, se debe utilizar una cámara fotográfica específica e identificada. La cámara debe estar siempre guardada bajo llave, y solo el personal autorizado debe manejarla. El registro fotográfico se realiza en concordancia a los requerimientos establecidos en los documentos. La memoria de la cámara solo debe ser manejada por el personal autorizado por la PMO del proyecto satelital, y solo algunas personas pueden acceder a las fotografías. En la figura de arriba se muestra un diagrama de flujo general el cual muestra el proceso de registro fotográfico del satélite. Este es un punto crítico en el manejo de la seguridad de la información para satélites, porque por medio de esos registros fotográficos se pueden reversar algunas tecnologías referentes a ejecución de pruebas, tipo de materiales usados, tipos de carga útil satelital, entre otros.

X. Conclusión

En este documento se ha realizado una revisión general de los lineamientos usados en el manejo de la seguridad de la información, específicamente se ha mencionado los lineamientos usados en el área satelital. De una revisión de este documento se puede desprender que los datos que son confidenciales deberían reposar en computadores que nunca deban estar conectados a redes abiertas. También se desprende que para el intercambio de información sensible entre diferentes lugares se debería hacer uso de conexiones punto a punto de fibra óptica. También se puede concluir que la información no debería ser almacenada en unidades de almacenamiento masivo, sino en CDs. En esta era en que las grandes mayorías tienen acceso a teléfonos inteligentes, generan la necesidad de utilizar bloqueadores de señales de internet inalámbrico en sitios donde se están ejecutando procesos de manufactura tecnológica, tal como es el caso de los satélites. Adicional a lo arriba expuesto, se pueden plantear las siguientes conclusiones para el manejo de la seguridad de la información confidencial para instituciones, en este caso para la ABAE:

1) Se debe establecer la posición de Gerente de la Seguridad de la Información Satelital en la ABAE. Su responsabilidad sería la de preservar el activo más importante que tiene la agencia: la información.
2) Solo se puede intercambiar información entre el personal de la ABAE en las diferentes sedes de forma encriptada y por medio de redes de fibra óptica.
3) Todo el personal de la agencia debe ser entrenado en materia de manejo en la seguridad de la información, tomando como referencia las estrategias de confidencialidad empleadas en el proceso de desarrollo de los satélites VRSS-1, VRSS-2 y VENESAT-1.

Referencias

[1] ISO Tecnología de la Información Técnicas de Seguridad-Sistemas de gestión de seguridad de la Información-Requerimientos, IEEE Standard ISO 27001, 2007.
[2] SECNAV, Department of the Navy Information Security Program, M-5510.36, June 2006.
[3] ABAE-DFH, comunicación privada, 2017.

Arturo Rojas. (M'11) es miembro de la Agencia Bolivariana Para Actividades Espaciales. Está adscrito a la Unidad de Desarrollo de Productos y Procesos. Estudio Física en la Universidad de los Andes y luego prosiguió con estudios de maestría en Ingeniería Óptica y Eléctrica en Telecom-SudParis en Francia. También tiene un Master 2 en Sistemas de Comunicaciones en Altas Frecuencias de la Universidad de Marnee La Valle, también en Francia. Ha estado involucrado con el Centro de Investigación y Desarrollo Espacial de la ABAE, y es el Inspector en Ensamblaje e Integración del Satélite Sucre, a la par de formar parte de la Oficina de Gerencia del Programa de dicho satélite.