# Implantación del Sistema de Gestión de Seguridad de la Información en una empresa compleja

***Ing. Eduardo Carozo Blumsztein , Mgt, Cis***
Gerente de Seguridad de la Información - Antel
Profesor Facultad de Ingeniería
Universidad de Montevideo
ecarozo@um.edu.uy

**Resumen**. El presente documento analizará la implantación de un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO 17799:2000, en la Administración Nacional de Telecomunicaciones de Uruguay (ANTEL) y sus subsidiarias.

## I. INTRODUCCIÓN.

ANTEL es una Empresa de propiedad estatal, líder en todas las líneas de mercado de las Telecomunicaciones en nuestro país, con una facturación anual de más de seiscientos cincuenta millones de dólares, distinguida en la mayor parte de las encuestas de opinión entre las mejores Empresas nacionales, públicas o privadas.

Además de soportar la provisión de servicios de telefonía fija, celular y datos, desarrolla importantes actividades en TI, promoviendo el portal del Estado Uruguayo, y proyectos de educación en telecomunicaciones e informática en más de 1000 locales educativos distribuidos en Uruguay.

El proyecto que se expondrá ha sido denominado "Programa de Seguridad de la Información de ANTEL" el cual se realizó en sus fases iniciales con la asesoría de la firma PricewaterhouseCoopers, y ha sido clasificado como caso de éxito mundial por dicha consultora, incluyéndose también las acciones subsiguientes que la Gerencia de Seguridad de la Información de ANTEL ha adoptado, y los resultados principales a los que se ha arribado.

Se detallará el proceso de evolución del proyecto en el tiempo, desde la visión de los diversos sectores de la Organización, el líder del proyecto y Gerente de Seguridad de la Información y la visión de las Gerencias Tecnológicas de ANTEL, que tienen a su cargo la operación y mantenimiento de los diversos servicios de TI corporativos o especializados de la compañía.

El objetivo del trabajo consistirá en mostrar las principales dificultades que se enfrentan cuando se propone a una Organización compleja, distribuida y en competencia, un proyecto de cambio cultural tan importante como el implantar un Sistema de Gestión de Seguridad de la Información y cuales fueron los caminos que permitieron y permiten gobernar el cambio en forma permanente y proactiva, generando lecciones aprendidas que puedan ser relevantes para otras Organizaciones.
Finalmente se analizarán el cumplimiento de los objetivos propuestos y su aporte al desempeño de la Organización, globalmente en términos de eficiencia, eficacia, relevancia y competitividad.

## II. DESCRIPCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE ANTEL Y SUBSIDIARIAS

La Administración Nacional de Telecomunicaciones dispone de una infraestructura en Tecnología de la Información compleja y cambiante, con múltiples plataformas con alta cantidad de interconexiones debido a los tipos de servicios que la empresa brinda. Los intercambios de información entre los diferentes sistemas soportados por las mismas, son en ocasiones claves para la continuidad del negocio, y deben tener disponibilidad continua, debiendo asegurar la integridad y la confidencialidad.

La empresa ha ido creciendo en base a conocimiento especializado, existiendo 8 empresas subsidiarias y/o Divisiones diferentes en la organización que utilizan en forma intensiva servicios y sistemas informáticos. A modo de ejemplo se dispone de dos Mainframes, Equipos AS/400, más de 200 servidores sobre diferentes Sistemas Operativos, 60 Centrales digitales especializadas para telefonía celular y fija, equipos para soportar la infraestructura del mayor ISP de nuestro país, etc.

Se puede visualizar el impacto de la empresa y sus servicios en la comunidad nacional visitando su sitio web: www.antel.com.uy

## III. ANTECEDENTES

Las redes estaban (y están!!) creciendo a ritmos exponenciales, pero mucho más rápido está creciendo la complejidad inherente a su Administración. Esto provocaba cada vez menor capacidad de resiliencia de las distintas Divisiones de Antel. Cuando existía algún incidente de seguridad, las crisis involucraban mas cantidad de Divisiones y a su vez mas cantidad de personal especializado de cada una de ellas, lo que dificultaba la coordinación y por lo tanto el obtener una respuesta a los incidentes en tiempo y forma. La mayoría de los problemas se debían a inconvenientes en la comunicación dada por la dificultosa coordinación de las acciones de seguridad y la carencia de políticas y de estándares.

En ANTEL la decisión de implementar el Programa de Seguridad de la Información respondió a dos causas:

1. La Dirección necesitaba disponer de mayor gobernabilidad de las distintas Divisiones Tecnológicas de operación y,

2. Las Divisiones Operacionales, cuando ocurrían incidentes de seguridad relevantes, tomaban conciencia de la necesidad de establecer dicho programa para disponer de una mayor capacidad y efectividad de respuesta frente a los incidentes.

## IV. CREACIÓN DE LA GERENCIA DE SEGURIDAD DE LA INFORMACIÓN

En el año 2000 debido a recomendaciones de un informe prospectivo realizado por una consultora externa, y a solicitudes sistemáticas año tras año, de la firma auditora externa de los estados contables, que explicitaban la necesidad de designar un responsable de la Seguridad de la Información de ANTEL, la alta gerencia de ANTEL decidió entonces llevar adelante un programa para la implantación de la Seguridad de la Información.

El mismo tuvo como objetivo: **“Proveer a ANTEL de las directrices principales en cuanto a Seguridad de la Información desde el punto de vista corporativo, considerando aspectos conductuales y de Seguridad Lógica, Física y Ambiental que incidan en el ambiente IT, generando un marco para el desarrollo y aplicación de una Política de Seguridad Corporativa”**

El programa comenzó en el 2003, con la creación de la Gerencia de Seguridad de la Información, la designación de un responsable de la misma quien debía poseer una importante orientación al negocio, profundo conocimiento de gestión y promoción de sistemas de calidad orientados en las normas ISO 9000, formación en investigación y desarrollo de proyectos y capacidad de entender la tecnología; y la creación de un equipo técnico conformado por personas de sectores claves de la Empresa con alta experiencia en operación en las áreas de Informática, Desarrollo, Operación y Organización & Métodos.

Desde el inicio el equipo se conformó como una Unidad Ad Hoc, el Gerente del Proyecto y Especialistas de Seguridad con dependencia directa, con una clara vocación de gestión y gobierno de proyectos complejos multidisciplinarios. El mismo se ubicó en dependencia directa del Directorio de la organización, con estricta independencia de las áreas de Tecnología de la Información de ANTEL.

Para mejorar la capacidad de gobernabilidad del mismo, se inició el trabajo con un proceso de definición de la Misión y Visión de la Gerencia de Seguridad de la Información, que se enfocan en lograr una implantación de colaboración de los distintos proyectos que el cambio cultural propone, alineados con la estrategia de negocios de la Empresa.

**Misión de GSI**: "Apoyar el logro de los objetivos de la empresa garantizando la seguridad de la información, propia o ajena, requerida para la adecuada operativa de la misma, en un ambiente competitivo."

**Visión de GSI**: "Alinear la gestión de la seguridad con las mejores prácticas, normas y políticas internacionalmente aceptadas, promoviendo el compromiso y concientización de toda la organización en relación al tema."

Junto con esto, se inició un proceso de capacitación y entrenamiento del Equipo de Seguridad en la amplia temática de Seguridad de la Información, y necesidades y problemáticas internas de la Empresa asociadas entre otros temas con la Tecnología de la Información la cual es extremadamente compleja dado por los servicios soportados que exigen vertiginosos y constantes cambios e innovaciones.

Precisamente esta situación provocó en el Equipo una doble sensación de urgencia, primero fue necesario aumentar la comprensión en tiempo real de los cambios que se procesaban en la Empresa, y segundo era imperioso tener un grupo de directivas claras que brindaran orientación de los esfuerzos a emprender para cambiar la cultura imperante en la organización.

## V. DESARROLLO DEL PROGRAMA PARA LA IMPLANTACIÓN DEL SGSI

Los trabajos previos comenzaron "conociendo la Empresa" a través de la identificación de los Componentes del Sistema de Información los cuales servirían como base para el desarrollo del Programa de Seguridad en la misma. Esta tarea se realizó bajo un enfoque del tipo "top-down", en el cual se comenzaba con entrevistas al máximo responsable quien derivaba en subalternos las preguntas más específicas. El proceso requirió de más de 50 reuniones técnicas y gerenciales con diferentes actores de la empresa.

En etapas y mediante el relevamiento de diferentes tipos de información manejada por las distintas Divisiones de ANTEL se identificó:

- Sistema Crítico de Información
- Procesos e iniciativas del negocio
- Matriz de tecnologías y estrategias, indicando aspectos específicos de seguridad derivados de cada tecnología

- Lista de principales amenazas, riesgos y debilidades detectados (a nivel de negocios)
- Lista de principales amenazas, riesgos y debilidades detectados (inherentes a la estrategia tecnológica)
- Matriz de riesgos

Un tema que no se resolvió en ésta etapa, con el objeto de bajar la complejidad al relevamiento fue determinar en forma biunívoca el responsable de cada activo. Esto llevó a la necesidad de asignarlo luego, lo que provocó algunas conductas reactivas en las Gerencias Operativas.

De cada una de estas etapas se obtuvieron una serie de documentos para la aprobación del Directorio:

- Misión de ANTEL en relación a la seguridad
- Sistema de Información Crítico
- Clasificación de la Información
- Modelo de Seguridad
- Áreas de Riesgo

De esta forma y con la primer versión del documento de Políticas de Seguridad de la Información preparado y aprobado por el Directorio, daba comienzo la siguiente fase del Programa de Seguridad de la Información.
La estrategia para el desarrollo de la fase y liderar el proceso de cambio se basó cuatro vías principales:

1º Definir las Políticas de Seguridad de la Información según las normas ISO 17799:2000, con su correspondiente aprobación por parte del Directorio.

2º Constituir un Equipo multidisciplinario de mayor alcance, que oficie de "centro neurológico" y tenga como cometido inicial, autorizar todas las interconexiones que se necesiten entre las distintas plataformas de los servicios y redes, así como asesorar en soluciones tecnológicas que permitan integrar las mejores prácticas disponibles. Este equipo denominado Conysec, ha subsistido hasta el presente, según lo exigido en la norma BS-7799:2.

3º Generar un Plan de Divulgación, Capacitación y Entrenamiento de amplio alcance.

4º Desarrollar un tablero de control del Sistema de Gestión de Seguridad de la Información.
Toda la programación de la estrategia descripta se realizó siguiendo la metodología de proyectos de PMI (Project Management Institute), y bibliografía asociada

## VI. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El disponer de un grupo de Políticas aprobadas por el Directorio se reconocía como un paso principal para brindar dirección y alineamiento de los distintos actores, brindando legitimidad al Equipo de Seguridad para dirigir los esfuerzos de estandarización en temas de Seguridad de la Información.

Analizadas las diferentes posibilidades, se decidió proponer como Políticas de Seguridad de la Información las más exigentes posibles a cumplir, bajo un estudio detallado de costo-beneficio. Se era conciente de que esta propuesta provocaría una importante brecha (GAP) entre la situación inicial y la deseada descripta por las Políticas a ser adoptadas.
Luego de ser evaluadas por múltiples Divisiones y con el aval de la División Letrada, se logra la aprobación de las Políticas de Seguridad de la Información para ANTEL por parte del Directorio de ANTEL, el 4 de noviembre de 2004.

Es un documento extenso de aproximadamente 90 páginas con un profundo nivel de detalle de las mejores prácticas en securitización de los diferentes ambientes de TI, manejando todos los aspectos habituales de la citada norma.

## VII. APLICACIÓN DE LAS POLÍTICAS

Una vez aprobadas las Políticas de Seguridad de la Información, era necesario llevarlas a conocimiento de las diferentes Divisiones para su aplicación y posible mejoramiento de acuerdo a la realidad y necesidad de las diferentes áreas del negocio.

Se elaboró una estrategia para la creación paulatina de la cultura de la Seguridad de la Información. Para ello en primer lugar fue muy importante buscar el apoyo de las distintas Divisiones, a través de la creación de equipos multidisciplinarios permanentes o temporarios para proyectos, así como un importante Plan de Capacitación.

Esta planificación tenía el doble objetivo de sensibilizar y a su vez lograr el compromiso con el programa a través de la toma de conciencia de que la Seguridad de la Información, es un compromiso de todos y cada uno de los trabajadores de ANTEL.

Se han elaborado desde su promulgación y están vigentes más de 70 procedimientos de alto y medio nivel que la empresa ha adoptado para mejorar su alineación con lo establecido en dicha política. La difusión de los mismos se ha hecho a través de cursos presenciales (más de 800 participantes), publicación en la intranet de la organización, y la difusión realizada por los integrantes del Conysec en cada una de sus Divisiones.

Se han resuelto más de 300 consultas y emitido más de 40 informes de recomendaciones de mejora de Seguridad lógica, física y ambiental en el último año, lo que muestra la relevancia y pertinencia de las Políticas adoptadas.

Se han promulgado en Diciembre de 2006, la segunda versión de las Políticas de Seguridad de la Información de ANTEL, basadas en la ISO 17999:2005, orientadas a una mejor evaluación de riesgos de seguridad, con mayor atención en el manejo de incidentes y más alineadas con los controles establecidos en COBIT.

Esta revisión se ha llevado a cabo mediante el retorno que los integrantes de las Divisiones en el Conysec realizan a través de su participación, sugerencias de terceros para la implementación de procedimientos e infraestructuras y el propio expertise generado en la Gerencia como resultado de sus actividades.

## VIII. CONTROL DEL SGSI

La Gerencia de Seguridad de la Información ha diseñado y puesto en marcha desde enero 2006, un Sistema de Control del Sistema de Gestión de Seguridad de la Información, el cual se encarga de controlar, difundir y evaluar en forma continua el avance de las actividades sobre cuatro dimensiones:

1. Cumplimiento de Cronograma de Proyectos de Seguridad de la Información
2. Cumplimiento del Cronograma de Desarrollo de Procedimientos de Seguridad Corporativa
3. Cumplimiento del Plan de Auditoria de Sistemas de Información de ANTEL.
4. Cumplimiento de indicadores de tiempo de respuesta y cantidad de consultas de Seguridad de la Información.

Dicho Sistema de Control está asociado a la Compensación Económica por Desempeño de los integrantes de la Gerencia de Seguridad de la Información y se viene ejecutando con efectividad

100%, hasta agosto 2006 inclusive, estando supeditado a auditorías realizadas por la Gerencia de Auditoría Interna de ANTEL.

El mismo está basado en las propuestas de COBIT y los intereses particulares del Directorio y la Gerencia de Seguridad de la Información para medir la eficacia y eficiencia del sistema de Seguridad de la Información.

## IX. INTERACCIÓN DE LA GERENCIA DE SEGURIDAD DE LA INFORMACIÓN CON EL RESTO DE LA ADMINISTRACIÓN

La ubicación en el organigrama de ANTEL de la GSI, quedó con dependencia directa del Directorio de la misma, en el mismo nivel que Auditoría Interna y Gerencia General (de la cual dependen las Gerencia Operativas), facilitando de esta manera las tareas de auditoría de seguridad de los diferentes sistemas (estableciéndose de forma obligatoria un Plan anual de Auditoría de Sistemas), así como la implementación de proyectos claves en Seguridad y los procesos de capacitación.

La interacción entre la GSI y el resto de la Empresa es necesaria para:

• Controlar los activos críticos, para lo cual se trabaja con todas las Divisiones bajo un enfoque de Gestión de Riesgos de Negocio, (es una de las actividades encargadas a Seguridad Procedimental) realizando un relevamiento de información y sistemas, tomando las sugerencias del Conysec, los informes de las Auditorías de Sistemas de Información, las denuncias de incidentes y la participación activa de técnicos especialistas en seguridad en los nuevos proyectos de la Administración.

• Integrarse a los procesos existentes, para lo cual contar con una fluida interrelación entre los técnicos de GSI y los técnicos de las Gerencias Operativas es imprescindible. La misma posibilita detectar proactivamente dificultades técnicas al implementar nuevas soluciones, así como asesorar y difundir las nuevas disposiciones que por imperativos de negocio se van definiendo.
Para responder a estas necesidades se han desarrollado dos Equipos multidivisionales:

• CONYSEC (Conectividad con Seguridad)
• CSIRT: Centro de Respuesta a Incidentes Informáticos y de Telecomunicaciones de ANTEL.
Estos equipos proveen interacción, proactiva (Conysec), y reactiva (CSIRT), que junto con las auditorias, el sistema de atención de consultas, el plan de capacitación y las recomendaciones de Seguridad de la Unidad de Seguridad Procedimental constituyen redes de comunicación valuadas como muy efectivas.

## X. CONYSEC

La definición de este equipo técnico multidisciplinario, nació con la idea de disponer de un punto de entrada a la Gerencia de Seguridad de la Información de requerimientos de conectividad entre redes y sistemas, así como de un grupo consultivo que realice el análisis y recomendación basado en las mejores prácticas disponibles para dicha conectividad.

El mismo reporta a la Unidad Seguridad Procedimental, que tiene la función de registrar las lecciones aprendidas y difundirlas al resto de la Organización. En base a estos registros se realizan auditorias anuales de las conectividades autorizadas y su estado.

Para constituir este Equipo, se invitó a las Divisiones interesadas a participar activamente (ANTEL tiene 20 Divisiones aproximadamente), y se realizó el nombramiento de los técnicos más relevantes quienes aportan su visión considerando las necesidades de su respectiva División.

Fue necesario al inicio de la actividad del Conysec, explicitar que lo único que se admitían eran soluciones que contemplaran los mandatos de ANTEL como un todo, por encima de los intereses particulares de cada División. Esta imposición causó más de una deserción del grupo al principio, sin embargo a largo plazo, se sumaron nuevos técnicos con posiciones más alineadas.

Este grupo ha sido sin lugar a dudas uno de los elementos clave para la difusión y promoción del cambio cultural de la Organización, y se ha constituido en un grupo asesor de gran relevancia, puesto que asesora y coordina junto a la Gerencia de Seguridad de la Información, sobre las mejores prácticas en la provisión de servicios e interconexión de redes, elabora los documentos de respaldo a las soluciones técnicas, y da continuidad al proceso de cambio en las redes de ANTEL.

Al estar representadas todas las Divisiones de TI se llegan a soluciones de compromiso que son las más eficaces y eficientes disponibles en el momento de la toma de decisión. Este Equipo es también un potente difusor de las Políticas, procedimientos y estándares técnicos en las distintas Divisiones de la Administración.

Es de hacer notar que la asistencia a dicho grupo es por invitación, que no se obliga a la permanencia y a diferencia de otros comités ya tiene tres años de funcionamiento ininterrumpido a través de reuniones quincenales.

Consultados los técnicos han manifestado que las reuniones que se dan son altamente útiles para su trabajo y que la constitución del mismo provocó la caída del paradigma de las parcelas. Dichas conductas perjudicaban seriamente el desempeño, porque perdían la visión integrada de las redes y las necesidades derivadas de los procesos de negocio de ANTEL, y no podían compartir el conocimiento experto en seguridad informática.

## XI. CSIRT

Se ha constituido desde Noviembre 2005 a la fecha un Centro de Respuesta a Incidentes Informáticos y de Telecomunicaciones de ANTEL, con técnicos que varias Divisiones que han sido entrenados bajo la metodología del CERT/CC de la Carnegie Mellon.

Desde constituido ha coordinado aproximadamente 100 incidentes de seguridad que han impactado a las líneas de negocio de ANTEL y la velocidad de respuesta ha aumentado significativamente, pero además se han implementado en forma sistemática acciones de mejora que están bajando la cantidad de incidentes a los que la Organización está sometida.

Dicho Equipo depende de un Comité Ejecutivo integrado por el Gerente de Seguridad de la Información, el Gerente del área técnica de la subsidiaria de datos, y el Gerente del área técnica de la subsidiaria de celular.

Este Equipo lidera técnicamente junto con la Facultad de Ingeniería de la Universidad de la República, el proyecto de instalación del primer CERT nacional en Uruguay.
Se ha conseguido con el auspicio de CERT.br y AusCERT aplicar como integrante del FIRST (Forum of Incident Response and Security Teams), siendo el sexto equipo de Latinoamérica y el primero de Uruguay, que lo consigue.[5]

## XII. SITUACIÓN ACTUAL DEL PROGRAMA

Además de las ya descriptas, se iniciaron varios proyectos que han permitido difundir las actividades de la Gerencia de Seguridad en la Empresa, así como promover una importante disminución de las brechas de seguridad.

En la fase actual del Programa de Seguridad de la Información, se reúnen Proyectos de índole corporativo, algunos de los cuales son considerados proyectos de investigación de alcance Nacional por diversas Organizaciones Académicas y Empresariales.

A continuación enumeramos los que se consideran de mayor importancia:

1. Implementación del CSIRT de ANTEL
2. Proyecto de Control de Usuarios de ANTEL
3. Proyecto "Aseguramiento de Ingresos y Evaluación de Riesgos de negocio"
4. Plan de capacitación y entrenamiento en Seguridad de la Información.
5. Red de Interconexión
6. Hackeo ético de la red de equipos de la plataforma celular
7. Centro de respuesta a Incidentes de ANTEL y sus principales clientes.
8. Plan de continuidad de operaciones para ANTEL
9. Hackeo ético de la red de equipos de soporte de Internet a nivel nacional
10. Hackeo ético de los servidores web principales de ANTEL
11. Proyecto Accesos Remotos
12. Estándares para Desarrollo
13. Proyecto CERTUY, Centro de respuesta a incidentes Nacional en conjunto con la Facultad de Ingeniería de la Universidad de la República
14. Proyecto Análisis de Códigos, en asociación con la Facultad de Ingeniería y la Facultad de Ciencias en el marco del PEDECIBA Programa de Desarrollo de las Ciencias Básicas
15. Implantación ITIL en División Informática

## XIII. EVALUACIÓN DEL SGSI

Las primeras actividades de la Gerencia de Seguridad de la Información estuvieron enfocadas en conocer la Empresa a través de entrevistas.

Estas entrevistas se realizaron en su gran mayoría a personal gerencial, participando en varios casos –pero no en todos- personal técnico.

La GSI había "nacido" y gran parte de los empleados estaba en conocimiento de su existencia, pero no de su rol en la Empresa. Incertidumbres respecto a su accionar y a su participación en las tareas de las Áreas técnicas eran los principales comentarios que se podían escuchar en los pasillos.

El relevamiento de los activos de información permitió concluir que los trabajos de la GSI no eran inútiles y que la tarea que se estaba llevando a cabo en la primer etapa era muy importante para la Empresa. Como evidencia de la falta de concientización en Seguridad por parte de los participantes en este relevamiento se detectaron algunos casos cuando se recibían comentarios como:

- "No sabemos quien es el dueño de la información"
- "Ya todos lo saben, el dueño es la División Informática"
- "Sólo deben dedicarse a escribir las Políticas…"
- "Son los policías de la Información, todo hay que preguntárselo a ellos"

La clasificación de la información también permitió mostrar que no toda la información "es la más crítica" y que disponer de una visión global es primordial a la hora de defender los intereses de la Empresa.

El apoyo a la GSI por parte de técnicos de las Gerencias Operativas permitió acelerar el proceso conocimiento de las problemáticas existentes en la Empresa, así como temas técnicos. El

nacimiento del Conysec compuesto por personal multidisciplinario y multidivisional fue una consecuencia de esta participación externa.

Las políticas de Seguridad estaban aprobadas, y la GSI había comenzado a tomar participación en tareas que hasta el momento eran realizadas por las Gerencias Operativas.

La evaluación de la seguridad en nuevas solicitudes de interconexión entre redes de datos fue una de ellas. Esta participación fue considerada por varios Empleados de la Empresa como una "intromisión" en las tareas que ellos realizaban. Otros lo consideraron "acertado" debido a que les quitaba responsabilidad asociada a definiciones de seguridad que ellos antes realizaban cuando en realidad solamente debían realizar la implementación.

A pesar que GSI ya había comenzado a realizar definiciones, muchos empleados (técnicos y jefes) seguían sin conocer los nuevos procedimientos o las nuevas definiciones. Gran parte de este desconocimiento se debía a la ineficacia en los mecanismos de divulgación utilizados por la GSI.

No obstante las áreas técnicas han ingresado en un proceso de cambio, desde los diseñadores de sistemas y los desarrolladores, hasta los administradores de la infraestructura tecnológica, adoptando el cambio cultural que propone el nuevo modelo.

Es claro que trabajar pensando en seguridad es más costoso, tanto a la hora de diseñar e implementar un sistema, como a la hora de definir y mantener una infraestructura para el soporte de dichos sistemas. La definición o redefinición de algunos procedimientos y el seguimiento de estándares (ISO 17799, ITIL) esta ayudando en ésta tarea.

Luego de cuatro años de trabajo, la Gerencia de Seguridad de la Información es conocida por la gran mayoría de los empleados de la organización vinculados a TI, reconociendo que parte de los técnicos interactúan y participan fluidamente de sus actividades.

En algunos casos no se ha asumido aún la necesidad de interactuar con ella, para solicitar recomendaciones, o reportar incidentes; conocen su existencia pero no su "utilidad" en el proceso de mejora, la visualizan en una posición de control y auditoria, no de apoyo a la gestión.

Al día de hoy las áreas de TI están invirtiendo muchos recursos en seguridad, aunque las tareas finalizadas son escasas dado el poco tiempo que se ha tenido desde la vigencia de la nueva visión. Se percibe por parte de los técnicos en ocasiones que las Políticas de Seguridad son muy exigentes, y de difícil cumplimiento, sin embargo, la mayoría de los equipos trabajan duramente para conseguirlo y mantener la operativa de TI.

La difusión de las Políticas de Seguridad de la Información es un tema que no ha sido lo suficientemente difundido, existiendo aspectos técnicos que no han sido bien conocidos y por lo tanto provocando respuestas como "no conocía que esto estuviera reglamentado por la Política". Se han realizado ingentes esfuerzos de capacitación para la difusión de conductas específicas frente al accionar diario de los empleados de ANTEL, pero no se ha logrado aún que todos los actores tengan un real conocimiento de todos los aspectos que reglamentan las Políticas adoptadas.

Asimismo existe desconocimiento por parte de algunos empleados, sobre todo en áreas geográficas distantes. Se ha priorizado la capacitación del personal perteneciente a los niveles superiores de la Empresa, dejando relegados algunos niveles mas bajos que son los que realizan la operativa diaria y la manipulación de los datos. Consideramos que los mecanismos de divulgación masivos no han sido todo lo efectivos que se esperaba.

## XIV. CONCLUSIONES

La implementación del Programa de Seguridad de la Información, es un proceso de largo plazo que se va construyendo y modelando, considerando el avance del programa por demás satisfactorio, en términos de eficacia ya que el mismo ha tenido logros mucho mayores que los objetivos trazados en las planificaciones iniciales.

Es importante destacar que en cada momento la capacidad de negociación, entre las partes, ha representado un factor fundamental para el éxito de la implementación de dichas políticas y procedimientos.

La acción mancomunada de la Gerencia de Seguridad de la Información con el equipo multidisciplinario Conysec y el accionar del CSIRT, son claves para la interrelación de la GSI con las otras Divisiones de la Empresa.

La constitución del equipo (hoy 14 personas) de la Gerencia de Seguridad de la Información con carácter multidisciplinario fue clave para lograr uno de los mayores sucesos del proyecto, su relevancia para la Organización, puesto que a través de la profunda comprensión del estado de situación de la misma, ha logrado implementar acciones de securitización efectivas, con el apoyo firme de la Dirección y las Divisiones.

Es importante consignar que en la etapa de definiciones es imprescindible contar con ayuda de especialistas entrenados, típicamente asesores externos, que tengan reconocimiento por parte de las Gerencias del negocio, porque el confeccionar las respuestas correctamente elaboradas, lleva tiempo y esfuerzo significativo.

Los indicadores que permiten ponderar el avance exitoso son varios, siendo algunos de ellos los siguientes:

• A pesar del cambio de autoridades en el Directorio de ANTEL, el apoyo al programa siempre fue de interés del mismo y de la Alta Gerencia

• Se ha aprobado la Segunda versión de las Políticas de Seguridad de la Información, que han sido objeto de revisión continua por los diferentes actores de la Empresa

• Se han capacitado y entrenado más de 1000 funcionarios de ANTEL con respecto a Seguridad de la Información

• Se han definido, divulgado y puesto en funcionamiento procedimientos para implementar mejores estándares de seguridad y lograr el cumplimiento de buena parte de las políticas, en tiempos menores a los programados

• El equipo técnico multidisciplinario llamado “Conysec”, no es de participación obligatoria y sin embargo, ya tiene 4 años de actividad ininterrumpida

• Se han definido, y puesto en marcha múltiples proyectos tendientes a mejorar el desempeño de la organización en lo relativo a seguridad, lo que muestra la relevancia que el proyecto tiene para la organización

• Se reconoce a GSI como un único punto corporativo para el tratamiento de incidentes de seguridad de la Información y se están coordinando las respuestas a dichos incidentes, lo que es un índice claro de eficacia.

Un punto clave de éxito de éste Programa ha sido el apoyo constante de los distintos Directorios de la Organización, que basados en una relación de alta confianza profesional y buena comunicación han visualizado este Proyecto como un elemento que permite mejorar el Control Interno, aumentar la capacidad de la Administración de responder frente a los incidentes de seguridad y por ende dar mejor respuesta a sus clientes y disponer de una posición privilegiada en el mercado nacional. (ANTEL habitualmente ocupa el primer o segundo lugar desde hace 10 años, entre las Empresas con mejor imagen corporativa del Uruguay).

Aún queda camino por recorrer, procedimientos por escribir, estándares para definir, consultas para contestar, bajo la consigna de continuar mejorando nuestro SGSI en beneficio de ANTEL.

Entendemos que el proyecto está aportando significativamente a la competitividad de la empresa, tanto porque el mismo propicia una mejora de imagen derivada de un mejor comportamiento de la infraestructura, así como aumenta la protección de los activos de información de la empresa, que en las circunstancias actuales se encuentran seriamente amenazados por la competitividad en el sector.

**AGRADECIMIENTOS**

Queremos agradecer especialmente a los integrantes de los Equipos que han contribuido en el presente trabajo, en particular:

• Seguridad Internet de División Informática de ANTEL,
• CSIRT de ANTEL,
• Unidad Seguridad Procedimental de ANTEL.

**REFERENCIAS**

[1] Norma ISO 17799:2000
[2] Norma British Standard - BS 7799-2:2002
[3] Centro Interamericano de Investigación y Desarrollo del Canadá (CIID), “Análisis Institucional y de la Organización”
[4] John Kotter; “El Líder del Cambio”, ISBN:970-10-1470-7
[5] Sapag Chain; “Preparación y Evaluación de Proyectos”; ISBN: 9701042484;
[6] Project Management Institute (PMI); “PMBOOK”, ISBN: 0619063491
[7] PricewaterhouseCoopers; “Technology Forecast: 2002-2004: Emerging Patterns of Internet Computing; ISBN: 1-891865-06-4
[8] www.first.org
[9] Georgia Killcrece; Klaus-Peter Kossadowski, Robin Ruefle, Mark Zajicek, “Organizacional Models for Computer Security Incident Response Teams (CSIRTs)"
[10]Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakoski, Georgia Killcrece, Robin Ruefle, Mark Zajicek “Handbook for Computer Security Incident Response Teams (CSIRTs)”.