EL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN COMO INSTRUMENTO DE GESTIÓN

AUTORES

ALFREDO REYES (1)
GABRIELA MADERNI (2)
GABRIELA SILVA (2)

(1) GERENTE COORDINADOR DE LA OFICINA DE SEGURIDAD DEL BANCO REPÚBLICA ORIENTAL DEL URUGUAY
(2) GERENCIA DE GESTIÓN EMPRESARIAL, **LATU**

INTRODUCCIÓN

La seguridad de la información no se concibe sin un sistema de gestión y un gobierno efectivo. Este gobierno no debe presentarse meramente desde una perspectiva teórica, sino desde el punto de vista de su implementación. Será fundamental que un gerente de seguridad de la información incorpore los amplios conocimientos para un gobierno de la seguridad efectivo, así como los elementos y las acciones necesarias para desarrollar una estrategia de seguridad de la información y un plan de acción para su puesta en práctica. Intentaremos, entonces, definir estos desafíos y cómo realizarlos.

Qué se entiende por información o un activo de información? La información puede ser definida como *"El conjunto de datos dotados de algún significado y propósito."* Actualmente desempeña una función de gran importancia en todos los aspectos de nuestras vidas. La información se ha tornado un componente indispensable para la realización de procesos en todas las formas empresariales y organizacionales. Hoy existen innumerables compañías en las que la información es el negocio. Entre los participantes de mayor relevancia se cuentan, por ejemplo, Microsoft, Google y Yahoo. En varias organizaciones el término información se suele considerar de forma aislada: se la trata y utiliza prescindiendo de todo otro activo sin el que no tendría sentido y sería casi imposible de gestionar. Generalmente no se concibe el software como información, sin embargo, se trata de información en torno a cómo procesar lo que entendemos por información. Aun así, los medios en los que se resguarda, se opera, se extrae y los equipos que la procesan, parecen no intervenir en la gestión de la información. ¿Qué sería de la información si no dispusiéramos de tangibles para almacenarla, equipos que la soporten y programas que la procesen y hagan funcionar esos equipos? Es allí donde resulta imprescindible vincular lo que conocemos como información, un activo, con el resto de los activos necesarios para gestionarla.

Las organizaciones tradicionales han sufrido transformaciones radicales al llegar a la era de la información. Las artes gráficas, la industria de la imprenta, las obras de arte, incluso obras maestras, ya no son trazos físicos, sino bloques de información almacenados digitalmente. Parece difícil considerar que exista empresa u organización que haya permanecido ajena a este avance de la tecnología de la información.

Cualquier daño a la confidencialidad o integridad de la información puede ser devastador. También puede serlo el hecho de no contar con la información en forma oportuna. Se estima que en menos de 10 años las organizaciones trabajarán con información 30 veces más que en el presente. Sin dudas, la falta de protección de este activo llevaría inevitablemente a situaciones de caos absoluto al medio empresarial y organizacional y, cada vez más, es ineludible su gestión, su gobierno y, sobre todo, su control.

El gobierno de la seguridad de los activos de información (en adelante gobierno de la seguridad de la información) debe ser una parte integrante y transparente del gobierno global de las empresas u organizaciones, con el fin de tener continuidad en sus negocios.

¿Cuál es entonces la importancia de este gobierno? La creciente dependencia y los sistemas que procesan información, junto con los riesgos, beneficios y oportunidades que esos recursos representan, han transformado al gobierno de la seguridad de la información en una función vital en todo ámbito. En especial si se tiene en cuenta que las tecnologías de la información mejoran sensiblemente las posibilidades de negocio, con lo cual su seguridad añade un valor significativo al momento de minimizar riesgos y, consecuentemente, disminuir pérdidas derivadas de eventos relacionados a la seguridad.

Es decir, no es suficiente con transmitir a los empleados de las organizaciones los objetivos, misiones y visiones y pautar las condiciones que conllevan al éxito, sino que además se debe comunicar cómo se va a proteger la propia existencia de su negocio.

Esto indica que una estrategia organizacional clara en materia de preservación tiene igual interés que una estrategia organizacional de negocio.

Según conceptualiza Julia Allen, autora de la Guía de CERT (Computer Emergency Response Team), en su tratado "The cert guide to system and network security practices": "Gobernar para la seguridad de una empresa significa ver una seguridad adecuada como un requerimiento no negociable de permanecer en el negocio. Para lograr una capacidad sustentable, las organizaciones deben hacer que la seguridad de la empresa sea responsabilidad de los niveles directrices".

Varios conceptos básicos se espera que sean de dominio del gerente de seguridad de la información para que éste pueda implementar un gobierno efectivo y contemple el conjunto de las funciones que se requieren. Entre los principales conceptos que debe conocer y manejar un gerente de seguridad de la información, se hallan los siguientes:

Confidencialidad: preservación de la información dentro de los ámbitos de conocimientos definidos y autorizados.

Integridad: permite asegurar que la información no es modificada sin autorización.

Disponibilidad: tan importante como cuidar de su confidencialidad e integridad. Contar con la información en forma oportuna puede llegar a transformarse en la diferencia entre la continuidad y discontinuidad del negocio.

Asimismo, es preciso manejar preceptos de auditabilidad, autorización, identificación, autenticación, no repudio, gestión de riesgos, exposiciones, amenazas, vulnerabilidades, impacto, criticidad, sensibilidad, controles, contramedidas, políticas, estándares, procedimientos, clasificación y ataques, entre otros. En cuanto a las tecnologías de seguridad, el gerente de seguridad de la información debe conocer en profundidad:

- Firewalls
- Administración de cuentas de usuarios
- Sistema antivirus
- Herramientas anti spam
- Sistemas de identificación (biometría, tarjetas de proximidad y otros)
- Encriptación
- Accesos remotos seguros
- Firma digital
- Redes privadas virtuales
- Análisis forense
- Tecnologías de monitoreo

En la década de 1990 las organizaciones comenzaron a crear servicios dedicados a la gestión de la seguridad de la información (SI) y nombraron los respectivos gerentes de SI.

En muchos casos se crearon estructuras insertas en otras existentes y frecuentemente se tendía a incluirlas dentro de las áreas de tecnologías de la información (TI). Si bien no era del todo extraño que así fuese, esa estrategia no permitía realizar una adecuada segregación de tareas.

Ocurría que la seguridad cedía terreno a las urgencias de la gestión tecnológica y al estar subordinada a la misma jerarquía se imponía el concepto de productividad al de seguridad. En ocasiones, ni siquiera se llegaban a complementar. Las prácticas de desarrollo de sistemas prescindían durante la creación y ciclo de vida de un sistema de los requerimientos en materia de seguridad.

Con el tiempo se fue comprendiendo que para lograr que ambas áreas se complementasen debían encontrarse en diferentes líneas de dependencia jerárquica. Fue entonces cuando la SI comenzó el proceso de independencia de la TI.

Se crearon unidades independientes de estructura muy simple hasta otras de estructuras más complejas, dependiendo del tamaño de la empresa y organización. Una estructura de complejidad medio avanzada puede ser la que se representa en la Figura 1.

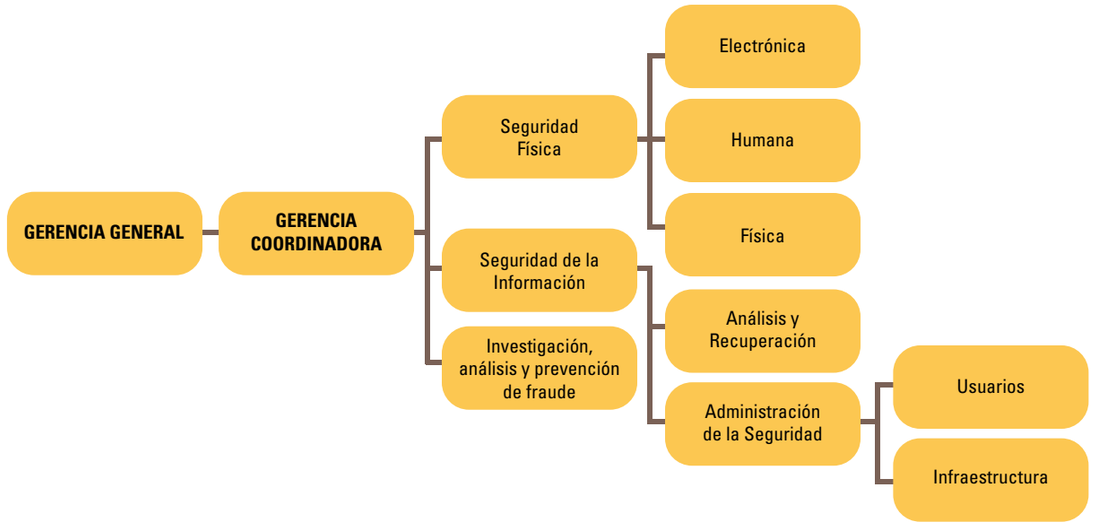

Figura 1. Organigrama modelo de una estructura de seguridad.

Un concepto preponderante y que debe ser muy bien gestionado por el gobierno de la seguridad de la información es que dicha seguridad debe tratar todos los aspectos de la información. Ya sea contenido escrito, oral, impreso, electrónico o constituida en cualquier otro medio sin importar si ha sido creada, vista, transportada, almacenada o desechada, siempre debe custodiarse. Obsérvese que no se está tratando la información solamente dentro del alcance de los límites o dominios tecnológicos. Un simple comentario en un pasillo podría estar divulgando información confidencial a personas no autorizadas para su conocimiento.

Para gestionar correctamente los activos de información es necesario que un buen gobierno de SI realice evaluaciones por lo menos anuales de la seguridad que los protege. Deben realizarse periódicos análisis de riesgos y existir políticas que sean revisadas periódicamente. Los procesos y procedimientos deben estar basados en esas evaluaciones de riesgos. Es esencial entender que la seguridad de los activos de información forma parte integral del ciclo de vida de los sistemas, probar los sistemas de control y protección de esos activos, y prevenir para asegurar una continuidad de las operaciones y, por ende, la continuidad de la organización en el negocio. Para hacerlo resulta de orden aplicar las mejores prácticas en materia de seguridad de la información, como lo puede ser alinearse a la norma internacional ISO/IEC 27001. Esta norma ha sido elaborada para constituir un sistema o modelo para la implementación, operación, seguimiento, revisión, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La norma ISO/IEC 27002 (nueva versión de la ISO/IEC 17799) constituye un código de buenas prácticas para la gestión de la seguridad de la información; complementaria de la anterior, aporta los requisitos para la implantación de aquélla. La norma ISO/IEC 27004 provee guías para el desarrollo y uso de medidas y mediciones, con el objetivo de evaluar la efectividad de un sistema de gestión de seguridad de la información. La norma ISO/IEC 27005 proporciona directrices para la gestión de riesgos de la Seguridad de la Información en una organización en apoyo a la aplicación de los requisitos planteados en la ISO/IEC 27001. En particular, esta última adopta un enfoque basado en procesos para el desarrollo de un Sistema de Gestión de Seguridad de la Información. Este modelo denominado PDCA (Plan, Do, Check, Act) es aplicado para estructurar todos los procesos del sistema de gestión.

La aplicación de estas normas requiere el diseño de una estrategia de SI. Son varias las definiciones de estrategia. Kenneth Andrews en su obra "El concepto de estrategia corporativa" (Andrews, 1997) propone que: "La estrategia corporativa es el patrón de decisiones en una compañía que determina y revela sus objetivos, propósitos y metas, genera sus políticas y planes para alcanzar sus objetivos, define su alcance en materia de Seguridad de la Información, el tipo de organización con que va a estructurarse y la naturaleza de contribución que aportará a la organización toda."

Por mucho tiempo se ha considerado erróneamente como un buen enfoque de una estrategia de seguridad el basado en la suposición de que un camino predecible en el futuro puede estar sustentado en las experiencias del pasado. En cambio, la estrategia que está marcando la realidad debe basarse en una cartera coherente y evolutiva de iniciativas que permitan agregar valor y desempeñarse a largo plazo; valiéndose de experiencias pero no basándose en ellas. Esto evidencia que las organizaciones se definen por las iniciativas que priorizan y gestionan y no sólo por sus declaraciones de misión y visión.

Cualquiera sea la estrategia de seguridad adoptada, los objetivos fundamentales consisten en:

- Alineación estratégica a la organización.
- Eficaz administración de riesgos.
- Entrega de valor.
- Administración de recursos.
- Medición del desempeño.
- Mejora continua.

Habitualmente, en toda organización lo más complejo de establecer en cuanto a la Seguridad de la Información es la meta. ¿Por qué es difícil esa definición? En verdad lo es porque, paradójicamente, resulta por demás obvio que lo que hay que proteger son los activos de información. Pero aunque esto resulte extremadamente simple, no lo es la determinación de los dos siguientes factores: el primero, que los activos de información deben conocerse con un alto grado de precisión, y esto comúnmente no ocurre en la mayoría de las organizaciones. El segundo factor es que se considera de conocimiento intuitivo lo que significa proteger un activo de información; dado que este concepto es entendido por cada persona en términos generales, se torna mucho más complejo cuantificar qué activos requieren protección, cuánta y contra qué.

La mayoría de las organizaciones no cuentan con inventarios de información o de los procesos que la gestionan. No se tiene noción en muchos casos de la información no utilizada, desactualizada o potencialmente riesgosa y no controlada. No existen procesos de eliminación. No tienen eficientes procesos de guarda. Todo se protege, ya que el almacenamiento es menos costoso que la clasificación de la información. No se distingue lo importante de lo no importante. Si suponemos que la información relevante que existe en la organización está debidamente identificada y catalogada, entonces no queda mejor alternativa que clasificarla. Esto se hará en función a su sensibilidad y criticidad. Se considera que una información es sensible cuando su divulgación no autorizada pueda ocasionar un severo impacto en la organización. En cambio, el concepto de su criticidad puede relacionarse más a la integridad y disponibilidad de la información. Sin lugar a dudas, un gran volumen de información en las organizaciones no es ni crítico ni sensible en el sentido dado. Tal vez sólo sea importante o medianamente importante. Por tanto, sería un derroche de recursos el resguardo igualitario de todo ese volumen. En definitiva, se invertirían demasiados recursos para protegerla.

En las grandes organizaciones clasificar los activos de información significa una tarea de enormes proporciones y un esfuerzo sustancial de muchos recursos. De no hacerlo, los costos asociados a la protección de esos activos crecerán de manera exponencial, al tiempo que aumentará la dependencia de la información. Por lo tanto, no hay mejor estrategia que realizar una clasificación.

En síntesis, el gerenciamiento de la seguridad de los activos de información no será efectivo y no tendrá la posibilidad de desarrollar una buena estrategia de protección según la demanda del negocio si antes no determina precisamente sus objetivos, si no localiza e identifica los activos y los evalúa, si no los clasifica y si no los protege de acuerdo a esa clasificación.

¿Cómo implementar un sistema de gestión de seguridad de la información y gobernarlo de acuerdo al paradigma propuesto?

Para que esto sea posible, la implementación del sistema de controles previsto por las normas mencionadas (familia ISO/IEC 27000) es de absoluta necesidad. Realizar una breve reseña de las normas, en particular de las ISO/IEC 27001 e ISO/IEC 27002 dotará a quien gobierne la seguridad de los activos de una organización de una aproximación a herramientas y estrategias fundamentales.

ISO/IEC 27001 y su aplicación en el contexto de una organización bancaria

El gobierno de la seguridad de la información requiere la implementación de directivas que ayuden a gestionar la seguridad de la información. Para ello es sustancial la aplicación de normas que garanticen el establecimiento, la implementación, la supervisión, la revisión y la mejora de la gestión de la seguridad de la información. En muchas ocasiones se constatan sistemas de información que no son seguros. ¿Por qué sucede esto? Porque las organizaciones no establecieron claramente los requisitos de seguridad.

Se hace imprescindible para las organizaciones la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que contemple la protección de sus activos contra amenazas, la confiabilidad, la seguridad y la disponibilidad de la información para asegurar la continuidad del negocio.

La norma ISO/IEC 27001 contempla los requisitos a cumplir para la gestión de la seguridad de la información. Dicha norma es aplicable a todo tipo de organización, desde industrias alimenticias, empresas desarrolladoras de software, estudios jurídicos o empresas públicas.

Como primer paso la organización debe definir el alcance del SGSI. Uno de los requisitos es que haya definido las metas y la dirección de la organización en lo que respecta a la seguridad de la información. Cabe destacar que no es suficiente con que la organización haya definido sus metas, sino que también debe considerar las políticas definidas en relación a la seguridad de la información, los requisitos contractuales y normativos y el marco legal en el cual está inmersa.

En ciertos casos, las organizaciones definen los activos pero no se identifican las amenazas a éstos, ni las debilidades que pudieran ser aprovechadas por dichas amenazas. En este sentido, otro requisito de seguridad es el análisis de riesgos. Por medio del uso de herramientas para este análisis se logra realizar una evaluación completa de los riesgos, incluyendo la estimación del nivel de riesgos, así como los criterios de aceptación de los mismos.

Al realizar el análisis de riesgo se cuenta con una gran cantidad de información que con frecuencia no es bien interpretada, de allí la importancia de la herramienta a usar. Para que el proceso de tratamiento de los riesgos sea efectivo, es preciso que esté basado en un completo análisis de riesgo. La información permitirá decidir cuál es el nivel de riesgo que se aceptará, qué riesgos serán tratados y cuál será el tratamiento para esos riesgos.

Esto implica la necesidad de definir un paquete de medidas que hagan posible controlar y tratar los riesgos. La norma ISO/IEC 27001 en su anexo A define objetivos de control y controles para el tratamiento de los riesgos. Estos controles no serán suficientes si no cubren todos los requisitos de seguridad de la información que definió la organización, por lo tanto es responsabilidad de la organización verificar si debe definir controles adicionales.

Todas estas medidas no serían válidas si no se obtuviese la aprobación y consentimiento de la dirección para la implementación del SGSI. Es asimismo responsabilidad de la dirección la aprobación de una política de seguridad de la información que definirá el ámbito de referencia para la fijación de los objetivos de seguridad de la información.

Siguiendo el modelo PDCA (Plan, Do, Check, Act), no alcanza sólo con definir controles si no se realizan un monitoreo y revisión del SGSI que permitan la detección de errores de proceso para luego tomar acciones que permitan corregir dichos desvíos, así como también poder implementar mejoras que se fueron detectando durante el proceso. La importancia fundamental de este modelo aplicado a un SGSI es que al planificar estamos previniendo, algo decisivo en lo que hace a la seguridad de la información.

Con base en los requerimientos de la organización en relación al alcance del proyecto se definió una metodología de trabajo para capacitación, evaluación y acompañamiento en la implantación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001.

Cómo se aplicó la norma con base en la realidad de la organización

Durante la realización del diagnóstico organizacional para detectar con qué requisitos de la norma de referencia dispone la organización bancaria y con cuáles no, se detecta que la norma ya se encontraba contenida en diferentes enfoques organizacionales y en las bases conceptuales de la organización. Tomando como base el modelo PDCA se diseñaron los procesos del Sistema de Gestión de Seguridad de la Información de la organización.

Se definió el alcance del SGSI, se revisaron las políticas de seguridad ya definidas y los objetivos de Seguridad de la Información. En pos de asegurar la eficacia y eficiencia del proceso de Seguridad de la Información, se identificaron los procesos del sistema, donde se definieron claramente el proceso de dirección, los procesos de realización y los procesos de apoyo, definiendo metas y objetivos para cada uno de éstos.

La herramienta usada, plan de calidad para la gestión de los procesos, permitió conjuntamente con una matriz de interacciones, establecer y gestionar la interacción con los procesos que se definieron.

Este modelo de procesos trajo como beneficios:

- La orientación de los procesos al beneficio de los clientes.
- Establecimiento de acuerdos claros en las interfases entre los procesos.
- Fácil adaptación ante cambios en los requerimientos.
- Transparencia para todos los involucrados.
- Consideración de los requerimientos de todos los grupos de interés.
- Menores costos y ciclos más cortos como consecuencia del uso eficiente de los recursos.

Los activos de información ya estaban definidos, se habían identificado las amenazas a éstos pero era necesario clasificarlos y establecer la periodicidad para realizar la identificación, análisis y evaluación de los riesgos. Para clasificar estos activos se contó con la participación de los dueños de los activos, lo cual redundó en un involucramiento del personal y en una clara definición de las amenazas de dichos activos: cuáles riesgos eran aceptados y cuáles no. En base a esta información había que definir cuáles

eran los objetivos de control y los controles que se debían aplicar para que cumplan con los requisitos identificados en el proceso de evaluación y tratamiento de los riesgos, tal cual lo exige la norma ISO/IEC 27001. La definición de un documento de aplicabilidad permitió realizar una revisión integral de la gestión que se estaba llevando a cabo sobre seguridad de la información, ya que permitió ver en detalle todos los controles que la norma exigía y obligó a verificar la procedencia y validez del conjunto de controles aplicados y cuán completos eran. Elaborar este documento ayuda a las organizaciones a detectar carencias que pudieran existir en todo lo relacionado a la gestión de la seguridad.

Implementar un buen sistema de medición de los procesos, usando como guía la norma UNIT ISO/IEC 27004 posibilita a las organizaciones la correcta evaluación del desempeño en todo lo referente al SGSI y, en base al análisis de las mediciones y a las sugerencias, realizar la mejora del SGSI.

Conclusiones

El éxito en la implementación de la norma ISO/IEC 27001, como modelo de gestión de la seguridad de la información en una organización bancaria, se fundamenta en que fue adoptada la norma y alineada a los objetivos y a lineamientos y necesidades especificas de la organización. Se constató que una adecuada administración es un fundamento muy importante para el gobierno de la seguridad de la información.

Este modelo colaboró en la reducción de los riesgos al ayudar a gestionarlos en forma segura y acorde a los requerimientos de la organización una vez que fueron establecidos los criterios contra los cuales se los evaluaría.

La definición de indicadores de gestión y medición de los procesos permitió evaluar la eficacia de los controles implementados. La evaluación de la necesidad de acciones que permitieron que las no conformidades no volvieran a ocurrir así como la implementación de las mejoras detectadas garantizaron el control en el funcionamiento y vigilancia efectiva de los procesos de seguridad de la información. Se logró validar que un enfoque basado en procesos para la gestión de la seguridad de la información, bajo un marco de responsabilidades y prácticas ejercidas en una dirección estratégica, asegura el alcance de los objetivos, el uso debido de los recursos y el control de los procesos que salvaguardan la información.

REFERENCIAS

ALLEN, J. *The cert guide to system and network security practices.* [s.l.]: Addison-Wesley Professional, 2001.

ANDREWS, K. El concepto de estrategia corporativa. En: MINTZBERG, H. *El Proceso Estratégico. Conceptos, contextos y casos.* México: Prentice Hall Hispanoamericana, 1997.

INSTITUTO URUGUAYO DE NORMAS TÉCNICAS (Uruguay). *UNIT ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requisitos.* Montevideo: UNIT, 2005.

INSTITUTO URUGUAYO DE NORMAS TÉCNICAS (Uruguay). *UNIT ISO/IEC 27002: Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.* Montevideo: UNIT, 2005.

INSTITUTO URUGUAYO DE NORMAS TÉCNICAS (Uruguay). *UNIT ISO/IEC 27004: Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Medición.* Montevideo: UNIT, 2009.

INSTITUTO URUGUAYO DE NORMAS TÉCNICAS (Uruguay). *UNIT ISO/IEC 27005: Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información.* Montevideo: UNIT, 2008.

NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY. *Special publication 800-100, information security handbook: aguide for managers. Information security.* Gaithersburg: NIST, 2006.

ENLACE RECOMENDADO

http://www.nist.gov

AGRADECIMIENTOS
Agradecemos a las siguientes personas por los aportes realizados: A/S Myriam Rodríguez Estades, Ing. Enrique Massonnier, Lic. Elke Enss, Sr. Damián Montans.