Aplicación de la Seguridad Informática como Herramienta de Gestión Empresarial en el Contexto del Gobierno TIC

Cadena Infante Andrés Felipe

andres-cadena2@upc.edu.co

Universidad Piloto de Colombia

RESUMEN

Las dinámicas de la sociedad han llevado a que la información sea manejada desde las bondades de las tecnologías de la información (TI); en ese sentido y dado el crecimiento del mundo digital y los volúmenes tan grandes de la información, se hace necesario el tratamiento, manejo y resguardo de la misma, tanto así que las instituciones que emiten normas a nivel mundial como la ISO y a nivel local como Icontec, han destinado espacios importantes a fin de parametrizar las formas del tratamiento de datos digitales, acompañando no solo el buen manejo de la información, sino de estandarización a fin de mantener una línea de acción especifica. A partir de lo anterior y en el entendido del cuidado de datos al interior de las empresas es que se ha definido el gobierno TI, como medio para transversalizar los lineamientos del manejo de información al interior de la organización y como herramienta en la toma de decisiones y eficiencia corporativa.

Palabras clave; gobierno TI, seguridad informática, gestión empresarial, normas.

ABSTRACT

The dynamics of society have led to information being managed from the benefits of information technology (IT); In this sense, and given the growth of the digital world and the large volumes of information, it is necessary to treat, manage and safeguard it, so much so that the institutions that issue standards worldwide such as ISO and locally such as Icontec , have allocated important spaces in order to parameterize the forms of digital data processing, accompanying not only the good management of information, but also standardization in order to maintain a specific line of action. Based on the above and with the understanding of data care within companies, IT governance has been defined as a means to mainstream the guidelines for information management within the organization and as a decision-making tool. and corporate efficiency.

Keywords; IT governance, computer security, business management, standards.

I. INTRODUCCIÓN

A nivel mundial, las tecnologías de la información se han convertido en un elemento esencial tanto en la economía como en el manejo del relacionamiento humano, pues la tecnología transversaliza absolutamente todas las dinámicas en el mundo. Adicional a lo anterior, el mundo virtual representa un factor de desarrollo en razón a que se ha ganado un papel importante para el control de los gobiernos en razón a que mejora la apertura de espacios de participación, lo que sirve como elementos de control de los gobiernos, pues permite una mayor participación indistintamente de la situación geográfica de los participantes.

Por otra parte, un grupo de gobierno al interior de una empresa en donde se involucren factores de seguridad en la información permitirá coordinar las actividades entre los diferentes departamentos y por lo tanto establecer prioridades, direccionamiento de la información al igual que las funciones, la facilidad en la toma de decisiones, participación del personal y eficiencia institucional.

A partir de lo anterior, el presente documento realiza un análisis sobre la importancia

de la aplicación de la seguridad informática como herramienta de gestión empresarial en el contexto del gobierno TIC, para ello el artículo se estructura en dos ejes fundamentales: el primero sobre el Gobierno TIC, y el segundo sobre el abordaje de la seguridad informática como herramienta de gestión en el gobierno TI.

II. GOBIERNO TIC

A. Contexto

La evolución de la tecnología ha permitido un avance a nivel mundial, no solo en la forma de comunicarse, de relacionarse, de negociar, sino que ha generado un dinamismo desde una mirada evolutiva del ser humano y su entorno, es por ello, por lo que las empresas y los Estados dependen hoy día de las tecnologías de la información (TI) para su desarrollo y buen funcionamiento.

En este sentido, las entidades realizan grandes esfuerzos e inversiones en TI buscando siempre ser más eficientes, más seguras, cumplir con la misión orientando estos aspectos al cumplimiento de la planeación estratégica; sin embargo, muchas empresas funcionan a modo de silos, aisladas unas de otras, las dependencias no se comunican y los esfuerzos de un área no se hacen evidentes, pues son desconocidos por el resto de la organización. Ross y Weil [1]manifiestan que una de las áreas más claramente afectadas es el de las TI, la cual puede plantear objetivos claros, pero estos no necesariamente están alineados con los objetivos del negocio.

Ahora bien, el concepto de gobierno de tecnologías de información (TI) lo explica Verhoef [2] como una estructura de relaciones y procesos para dirigir y controlar la función de dichas tecnologías de una organización con el fin de alcanzar sus objetivos mediante la agregación de valor y el equilibrio del riesgo y la consideración del retorno sobre TI y sus procesos. Parte del gobierno de TI consiste en diseñar, aplicar y evaluar un conjunto de reglas para gobernar la función respectiva en forma óptima.

En esta misma línea, Kim et al., [3], definen gobernanza de TI como una práctica o un grupo de actividades institucionalizadas que permite reducir la incertidumbre y lograr un mejor desempeño en la relación de subcontratación entre proveedores de servicios de TI y subcontratistas. Al respecto, Huang, et al., [4], establecen que el gobierno de TI puede definirse como la capacidad del consejo de administración y la dirección ejecutiva y de gestión para controlar la formulación e implementación de estrategias y asegurar la fusión exitosa de los negocios y la información.

En forma paralela, Rahimi[5]la define como un conjunto de objetivos, principios, organigramas, políticas y reglas que definen o limitan lo que pueden hacer los gerentes del área. Adicional a lo anterior, Muñoz y Villegas [6] considera que el gobierno de TI hace parte del gobierno empresarial y se define como la estructura de relaciones y procesos para dirigir y controlar la organización hacia el logro de sus objetivos por medio del valor agregado, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos al integrar e institucionalizar las buenas prácticas para garantizar que las TI en la compañía soporten los objetivos del negocio y facilitar que la empresa aproveche al máximo su información mediante la maximización de los beneficios, la capacitación de las oportunidades y el aprovechamiento de las ventajas competitivas.

B. Gobierno TIC y gobierno corporativo

El avance tecnológico por el que ha pasado la humanidad ha involucrado no solo la vida de las personas al interior de sus hogares, también desde el ámbito laboral en donde las TI son cada vez más el eje fundamental que engrana todas las áreas de la empresa.

Ahora bien, es importante tener claridad que la tecnología se apodera cada vez más del mercado, por lo que el área de la TI representa un apoyo fundamental que es transversal a todas las operaciones de la empresa que además interactúan dentro de las unidades del negocio. Es así como Valencia et al [7] argumentan que es necesario contar con un adecuado gobierno de TI, entendiéndolo como aquel órgano de alto nivel que

toma las decisiones cuyo rol principal es la evaluación, dirección y supervisión de las tecnologías de la información.

En este orden de ideas es importante señalar que estas actividades tienen un inicio trascendental, el cual se direcciona en comunicar a los altos mandos empresariales, la necesidad de gestionar y gobernar las TI y que tengan total claridad que esto no corresponde a un método aleatorio, ni por regulación, más bien para comprender que permite tener un sentido común para hacer las cosas bajo una perspectiva de mejores prácticas y con el objetivo de generar valor a las diferentes partes interesadas de la organización; es precisamente a partir de ello que se encuentran algunas respuestas y se determina que realmente se puede tener modelos de gobierno de TI que facilitan manejar aquello que se pensó no era posible.

Sumado a lo anterior y teniendo como base las competencias y competitividad de la sociedad actual, la velocidad, la eficiencia de los recursos y más recientemente la ética en el manejo de los dineros públicos, aparecen la gobernanza y el buen gobierno como conceptos fundamentales para tratar de armonizar el mundo cambiante de las organizaciones. Es así como Navarra et al [8], manifiestan que la construcción de una economía dinámica, una sociedad y organizaciones de buen gobierno, implican esfuerzos para una nueva configuración, desde su reinvención, tratando de alinearse con las nuevas demandas que surgen de los interesados que se ven cada vez más a sí mismos como participes de una sociedad global.

En este sentido, Janssen y Voort [9] manifiestan que la gobernabilidad puede ser abordada analíticamente describiendo las instituciones como generadoras de patrones que rigen las actividades de los actores sociales, políticos y administrativos, enfatizando los procesos para guiar, dirigir, controlar o gestionar sectores o facetas de sociedades. En lo respecta a la gobernanza convencional, esta se refleja en recursos confiables creencia en el control de la información y poder. A partir de lo anterior se evidencia que el gobierno TI aborda nuevas formas de gobernar mediante información y los flujos de datos que se presentan en la era de la información. [7].

En esta misma línea Muñoz y Ulloa [10] explican que el gobierno corporativo comprende una serie de responsabilidades y practicas ejecutadas entre la gerencia y la junta directiva en donde se deben tener objetivos clave como: definir claramente una gestión estratégica, asegurar el logro de los objetivos, establecer que los riesgos se administran de manera adecuada y verificar que los recursos de la empresa se gestionan responsablemente.

Por su parte, Juiz, et al [11] argumentan que la gobernanza de TI tiene como objetivo la evidencia de que las tecnologías de la información es un activo estratégico y proporciona un valor importante a la empresa; en ese sentido, las actividades del gobierno de las TI incluyen una serie de mecanismos que buscan la alineación de las TI con los objetivos en el contexto de la actividad empresarial.

Uno de los mecanismos usuales para mejorar la alineación entre la junta, las unidades de negocio (solicitantes de proyectos de TI) y el personal de TI (adquirentes o desarrolladores de TI) es la transparencia en los procesos de aprobación de la cartera de proyectos [11], situación que si se da de manera efectiva debería promover que las empresas comunicaran una alineación entre los objetivos y proyectos de una forma efectiva, creando más valor de los activos de TI.

Lo anterior lo refuerzan Torres et al [12], al manifestar que el gobierno de las TI agrupa y apoya la institucionalización de buenas prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte, y monitoreo del rendimiento de TI a fin de asegurar que la información manejada y las tecnologías utilizadas soportan los objetivos estratégicos de tipo organizacional, es por ello que el gobierno TI lleva a la entidad a tomar ventaja de la información en logro de maximizar sus beneficios, capitalizar sus oportunidades y obtener una ventaja competitiva mientras se equilibran los riesgos y el retorno de inversión sobre TI y sus procesos.

Por lo mencionado, los esfuerzos para lograr un buen gobierno de TI, tiene como fin el afianzamiento de organizaciones exitosas y perdurables en el tiempo, generando valor a accionistas, clientes, proveedores y empleados. En ese sentido es importante resaltar que los esfuerzos para consolidar un buen gobierno de TI se deben realizar con el mínimo riesgo posible a partir de una correcta implementación de controles e indicadores que correspondan con las necesidades de la organización y sus objetivos estratégicos.

Resulta de gran importancia, resaltar a uno de los referentes más utilizados por la comunidad académica y profesional para establecer de manera explícita los elementos que hacen parte del gobierno de TI, la cual corresponde a la propuesta realizada por IT - Governance Institute[13] a través del marco de referencia COBIT 4.1, donde define como principales dimensiones del gobierno de TI, la alineación estratégica, entrega de valor, administración de riesgos, administración de recursos y medición del rendimiento. La alineación estratégica permite alinear las TI con el negocio. La entrega de valor ejecuta la propuesta de valor a través del ciclo de entrega de servicios de TI. La administración de riesgos permite proteger los activos, recuperarse de los desastres y cumplir con las leyes, regulaciones y contratos. La administración de recursos permite optimizar el desarrollo y uso de los recursos disponibles. Y por último la medición del rendimiento, monitorea los resultados para aplicar acciones correctivas. [13]

Prieto y Piattini [14] comentan que la mejora continua en el gobierno de la organización y las TI está directamente relacionado con factores asociados a comprensión entre ejecutivos de TI y otros ejecutivos; optimización en la toma de decisiones mediante el uso de información más oportuna y de mejor calidad; iniciativas de proyectos alineados a obligaciones de negocio; conformidad con otros requisitos reglamentarios, tales como privacidad; mejora en las operaciones con un enfoque integrado de seguridad, disponibilidad e integridad de proceso; gestión de riesgos optimizada y priorización más eficiente de las iniciativas de negocio y de TI.

Los aspectos anteriores indudablemente traerán beneficios asociados a la reducción de costos, mejora de desempeño, capacidad para reaccionar rápidamente a los cambios en el mercado, ya que es fácil reconfigurar los activos de TI; mejora en la satisfacción del cliente y las prácticas de buen gobierno, tal como lo manifiesta Valencia et al [7].

En esta misma línea se encuentran los pronunciamientos de Velázquez et al [15], los cuales manifiestan que para que se presente gobernanza de TI, sebe también estar presente la de orden corporativo, la cual define unas estructuras y se orienta a controlar el rendimiento a fin de asegurar que los objetivos se cumplan. La gobernanza de TI incluye la especificación del conjunto de derechos facilitando la toma de decisiones y favorece una buena práctica que apoye el uso de las TI.

Ahora bien, los administradores deben contar con herramientas que les direccionen una buena gestión en donde se tengan unos parámetros definidos que muestren orientación a las buenas prácticas, el cumplimiento de los objetivos y eficiencia corporativa. Es así como Muñoz y Ulloa [10], argumentan que de acuerdo con el informe de Alec Cram, el cual es considerado uno de los medios más eficaces para direccionar a la junta directiva sobre la gestión buscando la alineación de TI y de negocio, es importante que, en el cumplimiento del objetivo, se cree un vehículo para la gestión de informes a la junta directiva para que dentro del consenso se identifiquen falencias y se propongan alternativas. En ese sentido, se deben tener en cuenta factores como:

1) Alineamiento estratégico. Se enfoca en asegurar el enlace de los planes del negocio y de TI; en definir, mantener y validar la proposición de valor de TI y en alinear las operaciones de TI con las operaciones de la empresa. [10]

2) Entrega de valor. Se refiere a ejecutar la proposición de valor a través de todo el ciclo de entrega, asegurando que TI entrega los beneficios acordados alineados con la estrategia, concentrándose en la optimización de costos, y demostrando el valor intrínseco de TI. [10]

3) Administración de riesgo. Requiere:

- Conciencia de riesgo por parte de los directores superiores de la empresa.

- Un claro entendimiento del apetito de riesgo de la empresa.

- Un entendimiento de los requerimientos de cumplimiento.

- Transparencia sobre los riesgos significativos de la empresa.

- Implementar las responsabilidades de la administración de riesgos dentro de la organización. [6]

4) Administración del recurso. Se refiere a la inversión óptima y a la adecuada administración de los recursos críticos de TI tales como: aplicaciones, información, infraestructura, datos. [10]

5) Medición del desempeño. Da seguimiento y supervisa la estrategia de implementación, la finalización de proyectos, el desempeño de procesos y la entrega de servicio. Si no hay forma de medir y evaluar las actividades de TI, no es posible gobernarlas ni asegurar el alineamiento, la entrega de valor, la administración de riesgos y el uso efectivo de los recursos [10]

A partir de lo anterior, se realiza el planteamiento de cuatro perspectivas según el IT BSC, tal como lo argumenta Cram [6], dentro de la cual el diseño esta ajustado para responder a la inquietud sobre la forma de hacer negocios de la empresa buscando una alineación entre la TI y el negocio. Las perspectivas son:

1) Financiera
2) Cliente
3) Interna
4) Aprendizaje y Crecimiento

Estas perspectivas están orientadas en:

- Proveer buen retorno sobre la inversión en las inversiones del negocio habilitadas por las TI.

- Administrar los riesgos del negocio relacionados con TI.

- Incrementar el gobierno corporativo y la transparencia.

- Mejorar orientación y servicio al cliente.

- Ofrecer productos y servicios competitivos.

- Establecer la disponibilidad y continuidad del servicio

- Crear agilidad en responder a requerimientos de cambio en el negocio.

- Obtener optimización de costos para entrega de servicios.

- Obtener información útil/confiable para toma de decisiones estratégicas.

- Mejorar/mantener la funcionalidad del proceso de negocio.

- Reducir costos de proceso.

- Proveer cumplimiento con leyes externas, regulaciones y contratos.

- Proveer cumplimiento con políticas internas.

- Administrar los cambios del negocio.

- Mejorar/mantener productividad operativa y del personal.

- Administrar innovación del negocio y de productos.

- Adquirir/mantener personal motivado y con destrezas. [10]

Finalmente, se destaca lo argumentado por Namén [7], el cual manifiesta que uno de los grandes inconvenientes del gobierno TI es poder

alinear los objetivos estratégicos con los de la organización, en donde desde una visión administrativa se pensaría que es una falta de planeación estratégica, pero realmente no solo es este factor el que se debe tener en cuenta, pues las áreas de TI al interior de las organizaciones están constantemente sometidas no solo a transversalizar su razón de ser en las instituciones, sino a mostrar resultados, además de las regulaciones técnicas y comerciales que ejercen presión y cumplimiento de parámetros, por ello el tener unos buenos lideres acompañado de un acertado equipo de trabajo puede hacer la diferencia en el éxito empresarial.

III. SEGURIDAD INFORMÁTICA COMO HERRAMIENTA DE GESTIÓN DEL GOBIERNO TIC

A. Seguridad de la Información

La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que ésta deba protegerse como el activo más importante de la organización. El empleo de herramientas tecnológicas de negocios en la operación empresarial ha impulsado la generación y la optimización de negocios en los ambientes empresariales, pero esto también ha generado la necesidad de concebir procesos que les permita salvaguardar la información ahora también digital. [17]

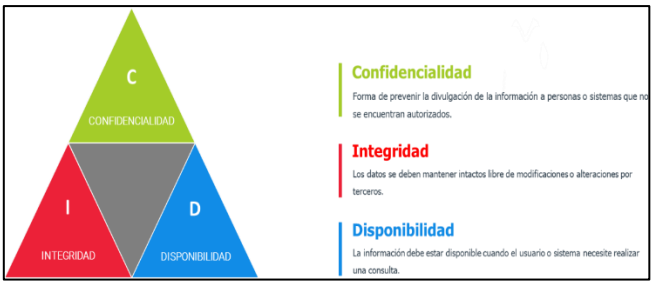

Fig.1 Pilares de la seguridad de la información

La seguridad de la información evidenciada en la figura 1 se desarrolla atendiendo a tres dimensiones principales, las cuales son, *confidencialidad* entendida como la garantía del acceso a la información únicamente de los usuarios autorizados, *integridad* como la preservación de la información de forma completa y exacta y *disponibilidad* como la garantía del acceso a la información en el instante en que el usuario la necesita. [18]

Para poder aplicar la seguridad de la información se han publicado importantes normas como la familia ISO 27000 y la NIST SP 800 que les entregan a los empresarios herramientas que a través de procedimientos que apoyan esta importante labor que es mantener segura la información.

B. Sistemas de gestión de seguridad de la información

Un sistema de gestión de seguridad de la información -SGSI- es parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Además, un SGSI a partir de la definición publicada en la norma NTC ISO 27000 consiste en las políticas, procedimientos, directrices y recursos y actividades asociados, administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información; también se puede entender como un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales; que se basa en la evaluación del riesgo y los niveles de aceptación de riesgos de la organización diseñados para tratar y administrar de manera efectiva los riesgos. [19]

La norma NTC ISO 27000 determina los principales lineamientos para tener en cuenta en el diseño de un SGSI:

- La organización es consciente de la necesidad de seguridad de la información.

- La organización debe establecer roles y responsabilidades en torno a la seguridad de la información.

- La organización y las partes interesadas

deben ratificar el compromiso por la seguridad de la información.

- La organización debe identificar, valorar y gestionar los riesgos en seguridad de la información.

- La organización debe garantizar un enfoque integral para la gestión de la seguridad de la información.

C. Norma Técnica Colombiana ISO/IEC 27001:2013

La Norma Técnica Colombiana NTC ISO 27001 hace parte de la familia de la ISO 27000. Esta norma establece los elementos que se requieren para la implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información; también sugiere que para la implementación de un SGSI se deben adoptar procesos formales de seguridad de la información, así como también se deben definir roles y responsables para actividades específicas. Por otro lado, con el apoyo y respaldo de la alta gerencia se deben establecer políticas, planes y procedimientos para la seguridad de la información dentro de la empresa. [19]

En cuanto a la gestión de la seguridad mediante un ciclo PHVA, (Planear – Hacer – Verificar – Actuar), alcanza la mejora continua del sistema de gestión contando con la responsabilidad de conservar y mantener información documentada como respaldo. El ciclo PHVA consta de cuatro fases: En la figura 2 se ilustra el Ciclo PHVA.

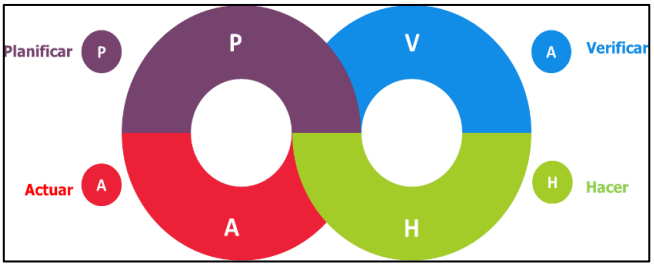

Fig. 2. Ciclo PHVA

- Fase Planificar. Dentro de esta fase establecen los objetivos del SGSI y las oportunidades de mejora, igualmente con los indicadores de medición para controlar y cuantificar los objetivos. [19]

- Fase Hacer: Se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas. [19]

- Fase Verificar: En esta fase del ciclo una vez implementada la mejora, se estipula un periodo de prueba para verificar el perfecto funcionamiento de las acciones implementadas. [19]

- Fase Actuar: Se analizan los resultados de las acciones implementadas y si estas por cualquier razón no se cumplen con los objetivos definidos, se analizan las causas de las desviaciones y se generan los respectivos planes de acción. [19]

D. Gestión del Riesgo

La planeación de un sistema de gestión de la seguridad de la información requiere una gestión de riesgos sistemática y acorde a las necesidades de la organización para que el abordaje sea eficaz y oportuno. Por lo que la norma NTC ISO 31000:2018, ha establecido los principios fundamentales que deben ser abordados para realizar el tratamiento de los riesgos, y con ellos suministra consecuentemente de una manera eficaz la respectiva gestión del riesgo. [20]

Se debe aclarar que la gestión del riesgo en la seguridad de la información debe ser un proceso continuo, tal proceso debe establecer el contexto, evaluar los riesgos y tratarlos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones, la gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable.

Para la gestión del riesgo es necesario tener en cuenta:

- Identificar los riesgos
- Valorar el riesgo
- Entender las consecuencias de la

materialización del riesgo.

- Establecer prioridades para el tratamiento del riesgo.
- Definir acciones de mitigación para los riesgos que lo requieren.
- Monitorear el tratamiento del riesgo.
- Documentar la gestión del riesgo.
- Realizar sesiones de sensibilización y capacitación de riesgos.

Para la planeación de un SGSI se desarrollan las actividades de establecimiento de contexto, valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo.

La identificación, análisis y valoración de los riesgos hacen parte de un sistema de gestión de riesgos, la norma técnica ISO 31000:2009 proporciona principios y directrices genéricas sobre la gestión de riesgos, además contiene lineamientos sobre cómo desarrollar estas actividades. El sistema de gestión de riesgos implica al igual que el SGSI la generación de políticas, procedimientos y actividades formales que permitan hacer seguimiento a los riesgos a los cuales la organización se enfrenta en su día a día.

Ahora bien, Brijalbo [21], manifiesta que la Norma técnica colombiana ISO/IEC 31000:2018 trata sobre la a identificación de los riesgos es una actividad que se debe desarrollar interactiva y permanentemente. La norma ISO 31000 recomienda considerar factores que está bajo el control y los que no están bajo el control de la organización, así como fuentes tangibles e intangibles; sin embargo, es de tener en cuenta que desde la norma se indica que es fundamental identificar con el riesgo sus causas, las vulnerabilidades y amenazas que le dan lugar en la organización. Además, se le suministra de manera continua el mantenerla bajo los lineamientos de la norma¸ ella le permite a la organización los siguientes resultados:

- Fomentar la gestión proactiva;
- Ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización.
- Cumplir con los requisitos legales y reglamentarios pertinentes y con las normas internacionales.
- Mejorar la presentación de informes obligatorios y voluntarios.
- Mejorar el gobierno.
- Mejorar la confianza y honestidad de las partes involucradas.
- Establecer una base confiable para la toma de decisiones y la planificación.
- Mejorar los controles.
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo.
- Mejorar la eficacia y la eficiencia operativa.
- Incrementar el desempeño de la salud y la seguridad, así como la protección ambiental.
- Mejorar la prevención de pérdidas y la gestión de incidentes.
- Minimizar las pérdidas.
- Mejorar el aprendizaje organizacional y
- Mejorar la flexibilidad organizacional.

De acuerdo con Brijalbo [21], aplicando la norma se asegura que la gestión del riesgo se entrelaza con la estructura y la cultura de la organización.

Por otra parte, la identificación, análisis y valoración de los riesgos hacen parte de un sistema de gestión de riesgos, la norma técnica NTC ISO 31000:2018 contiene lineamientos sobre cómo desarrollar estas actividades, mientras que el sistema de gestión de riesgos implica al igual que el SGSI la generación de políticas, procedimientos y actividades formales que permitan hacer seguimiento a los riesgos a los cuales la organización se enfrenta en su día a día.

E. Plan de tratamiento de riesgo

Una vez la organización identifica los riesgos a los que está expuesto debe establecer los criterios para determinar en qué medida puede aceptar estos peligros o, por el contrario, criterios de acción para mitigar dichos riesgos. En la evaluación de cada riesgo se debe elegir qué acciones tomar, estas acciones deben estar alineadas con las necesidades de la organización, pero también deben estar a la medida de sus capacidades operacionales y financieras. Estas

acciones se denominan controles. Aquí es importante el apoyo sobre lo que en este sentido menciona la norma NTC-ISO/IEC 27000 para el tratamiento de riesgos, en donde se debe tener en cuenta aspectos como:

• Aplicar controles apropiados para reducir los riesgos.

• Aceptar los riesgos a sabiendas y objetivamente, siempre que satisfagan claramente la política y los criterios de aceptación de riesgos de la organización.

• Evitar riesgos al no permitir acciones que causarían que ocurran los riesgos.

• Compartir los riesgos asociados con otras partes, por ejemplo, aseguradoras o proveedores. Para aquellos riesgos en los que la decisión de tratamiento de riesgos haya consistido en aplicar controles adecuados, estos controles deben seleccionarse y aplicarse.

F. Declaración de aplicabilidad

Durante las fases anteriores desarrolladas a partir de lo sugerido por la norma NTC-ISO/IEC 27001:2013 se debe lograr la identificación de los activos y su valoración, la identificación de los riesgos y su valoración y finalmente los controles para el plan de tratamiento de los riesgos. El resultado generado se convierte en los requisitos de seguridad de la información para el proceso de infraestructura de GSEIT y debe exponerse formalmente al interior de la organización mediante el instrumento de declaración de aplicabilidad.

A partir de lo anterior, la norma indica que los controles deben garantizar que los riesgos se reduzcan a un nivel aceptable teniendo en cuenta aspectos como:

• Los requisitos y limitaciones de la legislación y los reglamentos nacionales e internacionales.

• Objetivos de la organización.

• Requisitos y limitaciones operacionales.

• Su costo de implementación y operación en relación con los riesgos que se reducen, y restantes proporcionales a los requisitos y limitaciones de la organización.

• Sus objetivos de seguimiento, evaluación y mejora de la eficiencia y eficacia de la información.

• Controles de seguridad para apoyar los objetivos de la organización. Selección e implementación de controles.

• Debe documentarse dentro de una declaración de aplicabilidad para ayudar con los requisitos de cumplimiento.

• La necesidad de equilibrar la inversión en la aplicación y el funcionamiento de los controles con la pérdida es probable que sea el resultado de incidentes de seguridad de la información.

Se debe aclarar que los controles especificados en norma NTC-ISO/IEC 27001:2013 son reconocidos como las mejores prácticas aplicables a la mayoría de las organizaciones y se adaptan fácilmente para acomodarse a organizaciones de diversos tamaños y complejidades.

G. Políticas de la seguridad de la información

Para Valencia y Orozco [22], es importante garantizar el éxito de un sistema de gestión de la seguridad de la información para una organización, por lo que se debe contar con liderazgo y compromiso, no solo de la alta gerencia como siempre se resalta, sino también, del compromiso que se les atribuye a todas las personas que hacen parte de la organización, estos compromisos, estas responsabilidades y estas obligaciones deben estar plasmadas en políticas.

Estas políticas son documentos directivos donde se definen los objetivos, las necesidades, el alcance y las responsabilidades de la organización y las personas que hacen parte de ella con respecto a la seguridad de la información. Las políticas de seguridad de la información se deben construir

desde la misionalidad de la organización y su visión, como también, a partir y la regulación y normatividad propia del país donde se desarrollen sus actividades; el objetivo de las políticas de seguridad de la información es brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

La importancia de las políticas de seguridad es que tienen el mismo objetivo del sistema de gestión de la seguridad de la información y permitiendo proteger los elementos valiosos para la organización, sus activos de la información. Las políticas de seguridad de la información se convierten en las reglas que se deben cumplir al interior de la organización para garantizar que se realizan las acciones que se requieren para cumplir los objetivos de la organización y la normatividad vigente.

Las políticas se pueden clasificar en tres grandes grupos a partir su impacto en la implementación y los objetivos a alcanzar. Los tres tipos de políticas son:

- Políticas de primer nivel. Políticas generales para la organización.
- Políticas de segundo nivel. Políticas de sistemas.
- Políticas de tercer nivel. Políticas específicas.

Las políticas de seguridad generales son esas que se aplican a toda la organización, son creadas a partir de los altos niveles de la organización y la norma técnica colombiana ISO 27001 sugiere que debe incluir:

- Estrategia de negocio
- Reglamentación, legislación y contratos
- El entorno actual y proyectado de amenazas da la seguridad de la información

Y debe contener declaraciones referenciadas por:

- La definición de seguridad de la información, objetivos y principios para orientar todas las actividades relacionadas con la seguridad de la información.

- La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos.

- Procesos para manejar las desviaciones y las excepciones.

Por otro lado, la normatividad hace parte fundamental de las políticas de primer nivel, cada organización debe identificar la normatividad que le aplica a partir de su sector productivo y las generales que aplican a toda la ciudadanía natural y jurídica.

Las políticas específicas desarrollan temáticas puntuales requeridas para la operación de la organización, es decir, acciones necesarias que hacen parte o deberían hacer parte del día a día de la organización, como las directivas para usar los recursos y herramientas tecnológicas. Estas políticas establecen a partir de los controles que deben implementarse para la mitigación de los riesgos existentes para grupos o personas especificas dentro de la organización.

Estas políticas se deberían comunicar a los empleados y a las partes externas interesadas, en una forma que sea pertinente, accesible y comprensible para el lector previsto, por ejemplo, en el contexto de un “programa de toma de conciencia, educación y formación en la seguridad de la información.

IV. CONCLUSIONES

El gobierno TI y su gestión, permite a las organizaciones y las personas tener una ruta definida para optimizar sus recursos, manejar la información de manera acertada y fortalecer la sinergia entre departamentos.

No se puede desconocer la trascendencia de las TI en la forma como operan y se relacionan los Estados con los ciudadanos, además de los beneficios en factores como la transparencia, eficiencia y eficacia en la prestación de servicios públicos, así como en el fortalecimiento de la participación ciudadana, por lo que el “gobierno

digital" se a una política pública que transversaliza e impacta todos los sectores del Estado y por ende de la sociedad.

Cada vez es más claro que el mundo es en un alto porcentaje digital, por lo que es importante involucrar en estos avances a la mayor cantidad de ciudadanía, pues, aunque se han hecho grandes esfuerzos por ello, no se puede negar que un fragmento de la población aun esta relegada digitalmente.

REFERENCIAS

1] Ross, J., & Weil, P, «Six IT Decision Your IT People Shouldn't Make,» Harvard Business, https://hbr.org/2002/11/six-it-decisions-your-it-people-shouldnt-make, 2002.

2] Verhoef, C, «Quantifying the effects of IT-governance rules,» *Science of Computer Programming, ,* vol. 6, nº 2, pp. 247-277 DOI: 10.1016/j.scico.2007.01.010, 2007.

3] Kim, Lee, Koo & Nam , «The role of governance effectiveness in explaining IT outsourcing performance. International Journal of Information Management,» *Journal of Information Management* , vol. 33, nº 5, pp. 850-860, 2013.

4] Huang, Shen,Yen y Chou, «IT governance: Objectives and assurances in internet banking.,» *Advances in Accounting,* vol. 27, nº 2, pp. 406-414. DOI: 10.1016/j.adiac.2011.08.001, 2011.

5] Rahimi, Møller, y Hvam, «Business process management and IT management: The missing integration.,» *International Journal of Information Management,,* vol. 36, nº 2, pp. 142-154, 2016.

6] Cram, «The IT balanced scorecard revisited,» *Information system control journal,* vol. 5, nº 1, pp. 1-5, 2007.

7] Valencia, Marulanda y López, «Gobierno de las Tecnologías de la Información. Uso y Prácticas en las Entidades Públicas del Triángulo del Café, Colombia,» *Revista de Información Tecnológica* , vol. 29, nº 3, pp. 249-256 , 2018.

8] Navarra y Cornford, « Globalization, networks, and governance: Researching global ICT programs.,» *Government Information Quarterly* , vol. 36, nº 21, p. 35–41, 2009.

9] Janssen y Voort, «Adaptive governance: Towards a stable, accountable and responsive government.,» *Government Information Quarterly,* vol. 33, nº 11, pp. 1-5, 2016.

10] Muñoz y Ulloa, «Gobierno de TI – Estado del arte,» *Revista S y T,* vol. 9, nº 17, pp. 23-53 , 2011.

11] Juiz, Gómez y Barceló, «Business/IT Projects Alignment through the Project Portfolio Approval Process as IT Governance Instrument. Procedia -,» *Social and Behavioral Sciences,* vol. 67, nº 70, pp. 70-75, 2012.

12] Torres, Arboleda y Lucumí, «Modelo de gestión y gobierno de Tecnologías de Información en Instituciones de Educación Superior,» *Campus Virtuales,* vol. 3, nº 2, pp. 96-107, 2014.

13] IT Governance Institute, «COBIT 4.1. Rolling, Meadows,» USA, 2004.

14] Prieto y Piattini, «Propuesta de marco de mejora continua de gobierno TI en entidades financieras,» *Revista ibérica de Sistemas e Tecnologías de Información,* vol. 6, nº 15, pp. 51-67, 2015.

15] Velásquez, Puentes y Pérez, «Un enfoque de buenas prácticas de gobierno corporativo de TI,» *Revista Tecnura,* vol. 19, pp. 59-169 , 2015.

16] Namén,A, «El gobierno digital: modelo en el que confluyen el Estado y las TIC,» de *Las TIC y la Sociedad Digital: Doce años después de la ley*, Bogotá, Universidad Externado de Colombia , 2021.

17] Ladino, Villa y López, «Fundamentos de ISO 27001 Y su

Aplicación En Las Empresas,» *Scientia et Technica* , vol. 15, nº 47, pp. 334-339. https://revistas.utp.edu.co/index.php/revistaciencia/article/view/1177/669, 2011.

18] Acosta y Patiño, «Diseño del Sistema de Gestión de Seguridad de la Información (S.G.S.I) para el centro de datos de la personería de Bogotá D.C. bajo las normas NTC-ISO-IEC 27001:2013 y GTC-ISO-IEC 27002:2013,» UNAD, Colombia , 2017.

19] ICONTEC, «Instituto Colombiano de Normas Técnicas y Certificación. Norma Técnica NTC-ISO/IEC 27001, tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos,» Icontec, Bogotá, 2013.

20] Alexander, Diseño de un sistema de gestion de seguridad de informacion Optica ISO, Alfaomega, 2007.

21] Brijalbo, Diseño del sistema integrado de gestión NTC/ISO/IEC 27001 e ISO 31000: 2018 aplicado a la ley estatutaria 1581de 2012, Bogotá: Escuela Colombiana de Ingeniería Julio Garavito, 2018.

22] Valencia y Orozco, «Metodología para la implementación de un Sistemade Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» *Revista lbérica de Sistemas e Tecnologias de Informação,* vol. 6, nº 22, pp. 73-88, 2017.