Importancia del Gobierno TI, Ciberseguridad y Comunidades Digitales. (junio de 2023)

Andres Ricardo Cuervo Forero andres-cuervo4@upc.edu.co

Resumen – En este artículo se analiza la importancia del gobierno de TI, la ciberseguridad y las comunidades digitales en la actualidad. Se destaca el impacto de estas áreas en el logro de los objetivos y la continuidad del negocio, así como en la interacción, colaboración y participación de las comunidades. Se abordan temas como la alineación estratégica, la gestión de riesgos, la eficiencia operativa, la transparencia y responsabilidad, y la promoción de la innovación y adaptabilidad. Este análisis busca resaltar el valor y la necesidad de una gestión adecuada en el entorno digital en constante evolución.

Abstract – This article discusses the importance of IT governance, cybersecurity, and digital communities today. The impact of these areas on the achievement of the objectives and the continuity of the business, as well as on the interaction, collaboration, and participation of the communities, is highlighted. Topics such as strategic alignment, risk management, operational efficiency, transparency and accountability, and the promotion of innovation and adaptability are addressed. This analysis seeks to highlight the value and need for proper management in the constantly evolving digital environment.

Keywords: Gobierno TI, seguridad, Activo, información, Ciberseguridad, tecnología, confidencialidad, integridad, disponibilidad, riesgos, Comunidad Digital, desafíos, regulación, ISO.

I. INTRODUCCIÓN

En la era digital actual, la tecnología de la información desempeña un papel fundamental en la vida cotidiana. La información se ha convertido en el activo más importante para alcanzar objetivos y garantizar la continuidad del negocio. En este contexto, es crucial contar con un sólido respaldo desde la alta gerencia (Junta Directiva) que esté alineado con el gobierno de TI y ciberseguridad. Este respaldo permitirá impulsar la innovación, mejorar la eficacia y ofrecer servicios adecuados a los clientes.

El gobierno de TI y ciberseguridad también beneficia a las comunidades digitales, ya que estas desempeñan un papel crucial en la interacción, la colaboración y la participación. Por lo tanto, es responsabilidad del gobierno de TI y ciberseguridad establecer políticas, procedimientos, lineamientos y otras medidas que aseguren la confidencialidad, integridad y disponibilidad de la información.

En este artículo, exploraremos el concepto de Gobierno de TI, las comunidades digitales y la importancia que esto implica en el mundo actual en el que vivimos.

II. GOBIERNO TI

La gobernanza de TI se define como la estructura de relaciones y procesos destinados a dirigir y controlar una empresa con el objetivo de lograr sus metas mientras se agrega valor y se busca un equilibrio entre el riesgo y el retorno de las inversiones en tecnología de la información y sus procesos [1].

En este contexto, resulta fundamental establecer políticas, procesos y lineamientos que garanticen la alineación de las inversiones en TI con las necesidades y objetivos de las empresas. Esto implica evaluar de manera continua las oportunidades y los riesgos asociados a la adopción y utilización de tecnología, así como implementar mecanismos efectivos de control y supervisión.

Además, la gobernanza de TI también abarca la definición de estrategias y la toma de decisiones relacionadas con la gestión de la información y los recursos tecnológicos. Esto incluye la optimización de los procesos, la seguridad de los datos, la gestión del ciclo de vida de los activos de TI y la gestión de proveedores y socios tecnológicos.

Con esto, la gobernanza de TI desempeña un papel crucial en el éxito y la sostenibilidad de las empresas en un entorno cada vez más dependiente de la tecnología. Al establecer políticas y procesos efectivos, se asegura una adecuada gestión de los recursos y una dirección estratégica que permita a las empresas alcanzar sus objetivos de manera eficiente y segura.

III. IMPORTANCIA DEL GOBIERNO TI

El gobierno de TI abarca diferentes aspectos que son fundamentales para el éxito y la sostenibilidad de las empresas en la era digital. A continuación, se explorarán algunos de estos aspectos:

Alcance estratégico: Una de las funciones clave del gobierno de TI es permitir a las empresas alinear sus estrategias de TI con sus objetivos generales. Esto asegura que las inversiones tecnológicas se dirijan hacia proyectos que aporten valor y contribuyan a la expansión y éxito de la empresa. Al tener una visión estratégica clara, las organizaciones pueden maximizar el impacto de sus inversiones en tecnología.

Gestión de Riesgos: Un gobierno de TI fuerte es fundamental para identificar y gestionar los riesgos asociados con el uso de la tecnología. Esto incluye la protección de datos, la ciberseguridad, el cumplimiento de las normas y la continuidad del negocio. El gobierno de TI establece procedimientos y controles para reducir y/o mitigar los riesgos, garantizando así la seguridad y la integridad de los activos de información de la empresa.

Eficiencia operativa: El gobierno de TI también desempeña un papel importante en la optimización de los procesos y operaciones internas de las organizaciones. Mediante la implementación de mejores prácticas, la estandarización de procesos y la adopción de tecnologías que automatizan tareas, las empresas pueden aumentar su eficiencia operativa y mejorar la productividad de sus empleados. Esto se traduce en ahorro de costos y mejoras en la calidad de los servicios.

Transparencia y responsabilidad: Un aspecto esencial del gobierno de TI es fomentar la transparencia en el uso de los recursos de TI. Esto implica rendir cuentas y difundir la información pertinente a todas las partes involucradas, incluido el público en general. La transparencia y la responsabilidad son fundamentales para generar confianza en el uso de la tecnología y establecer relaciones sólidas con los clientes, proveedores y socios comerciales.

Innovación y adaptabilidad: El gobierno de TI no solo se ocupa de mantener las operaciones actuales, sino también de promover la innovación y la adaptabilidad a los cambios en el entorno digital. Esto implica fomentar la investigación y el desarrollo de nuevas soluciones tecnológicas, así como estar al tanto de las tendencias y avances en el campo de la tecnología. La capacidad de adaptarse rápidamente a las nuevas demandas del mercado es crucial para que las organizaciones se mantengan actualizadas y sean competitivas.

Es así, como el gobierno de TI desempeña un papel integral en el manejo estratégico de la tecnología en las empresas. A través de la alineación estratégica, la gestión de riesgos, la eficiencia operativa, la transparencia y responsabilidad, y la promoción de la innovación y adaptabilidad, las organizaciones pueden aprovechar al máximo sus inversiones en tecnología y mantenerse relevantes en un entorno empresarial en constante evolución.

IV. ÁREAS DE ENFOQUE DEL GOBIERNO DE TI COBIT

En este artículo, se aborda la importancia del gobierno de TI, haciendo hincapié en el marco de referencia COBIT [2] para comprender las áreas clave en este proceso. (Ver figura 1. *Áreas focales establecidas por el marco de referencia de COBIT*)

Figura 1 Áreas focales establecidas por el marco de referencia de COBIT

El primer aspecto es el *Alineamiento Estratégico*, que se refiere a la consistencia y coherencia entre el plan estratégico, la cultura y las actividades de ejecución.

La *Entrega de Valor* es otro aspecto crucial, donde cada elemento del cronograma del proyecto está asignado a una partida presupuestaria, lo que permite cuantificar el progreso financiero a medida que avanza el tiempo.

Asimismo, la *Gestión de Riesgo* es esencial para identificar, medir y administrar los riesgos que amenazan a la organización, sus activos, ganancias y personal, así como los servicios que ofrece.

La *Gestión de Recursos* implica la administración efectiva de diversos recursos limitados, como tecnología, finanzas, tiempo y personal, utilizando criterios eficientes.

Por último, la *Medición de Desempeño* es clave para evaluar la eficacia, eficiencia y adaptabilidad de las acciones. Proporciona información para la toma de decisiones tanto para directivos como para empleados.

Estos aspectos del gobierno de TI, delineados por COBIT, son fundamentales para garantizar una gestión efectiva y alineada con los objetivos estratégicos de la organización.

V. CONOCIMIENTO DE LA EMPRESA

Es crucial comprender el proceso de diagnóstico como el primer paso para implementar un buen gobierno de TI en una empresa. Para ello, se deben conocer los grupos de interés, identificar los macroprocesos y procesos de la compañía, lo

que permitirá evaluar con éxito el estado del gobierno de TI. Factores como el tamaño de la organización, su actividad económica y su plan estratégico corporativo también deben ser considerados en este proceso de diagnóstico [3]. Utilizando esta información, se puede realizar una evaluación de los controles existentes y elaborar un plan de trabajo que aborde las debilidades identificadas.

El gobierno de TI, en esencia, busca integrar e institucionalizar las mejores prácticas para asegurar que la tecnología de la información en la empresa respalde los objetivos del negocio. Su propósito es permitir que la organización aproveche al máximo su información, maximice los beneficios, capitalice las oportunidades y obtenga ventajas competitivas [4].

En cuanto a las responsabilidades, se establece que la Junta Directiva y la Gerencia Ejecutiva son las principales responsables del gobierno de TI. Según el Instituto de Gobierno de TI, existen cuatro principios fundamentales que deben ser considerados en este proceso: dirigir y controlar, responsabilidad, rendición de cuentas y actividades [3].

El análisis y la implementación adecuada de estos principios permitirán establecer una sólida estructura de gobierno de TI en la empresa, asegurando una dirección estratégica efectiva y un control adecuado de las actividades relacionadas con la tecnología de la información. El gobierno de TI desempeña un papel fundamental en el logro de los objetivos empresariales y en la maximización de los beneficios en un entorno cada vez más digitalizado y competitivo.

VI. GOBIERNO DE CIBERSEGURIDAD

El gobierno de ciberseguridad es el conjunto de políticas, estrategias y acciones implementadas por una organización o gobierno con el objetivo de proteger sus sistemas de información y redes contra amenazas cibernéticas. En un entorno digital cada vez más complejo y conectado, es fundamental contar con un enfoque integral para salvaguardar la confidencialidad, integridad y disponibilidad de la información y los sistemas.

Éste se centra en la protección de los pilares fundamentales de la seguridad cibernética. Estos pilares incluyen la confidencialidad, que garantiza que la información solo sea accesible para las personas autorizadas; la integridad, que asegura que la información no sea modificada de manera no autorizada; y la disponibilidad, que se refiere a la capacidad de acceder a la información y los sistemas cuando sea necesario.

Para lograr una efectiva gestión de la ciberseguridad, se deben establecer políticas claras y adecuadas, diseñar estrategias de prevención y respuesta ante incidentes, implementar medidas de seguridad técnicas y organizativas, y promover la concientización y capacitación del personal en materia de seguridad cibernética.

El gobierno de ciberseguridad también implica la identificación y evaluación de riesgos, la adopción de medidas de mitigación y la implementación de controles de seguridad adecuados. Esto incluye la protección contra ataques cibernéticos, intrusiones, robo de datos, sabotaje y otros riesgos relacionados con la seguridad de la información.

Con esto, es importante comprender que el gobierno de ciberseguridad es esencial para garantizar la protección de la información y los sistemas de una organización frente a las constantes amenazas cibernéticas. Mediante la implementación de políticas, estrategias y acciones adecuadas, se busca mantener la confianza de los usuarios, proteger los activos digitales y asegurar la continuidad de las operaciones en un entorno digital cada vez más desafiante.

VII. DIFERENCIA ENTRE GOBIERNO DE TI Y CIBERSEGURIDAD

El gobierno de TI y la ciberseguridad son dos conceptos relacionados, pero con enfoques distintos. Mientras el gobierno de TI se centra en la gestión de los recursos de tecnologías de la información, el gobierno de ciberseguridad se orienta específicamente hacia la protección de los sistemas e información contra amenazas cibernéticas y vulnerabilidades. Aunque diferentes, ambos conceptos son complementarios y se necesitan mutuamente para garantizar un entorno de TI seguro y efectivo.

La estrategia de seguridad en el contexto de la ciberseguridad es fundamental para lograr los objetivos del negocio. [3] (Ver figura 2. *Estrategia alineada a los objetivos*). Proporciona la base para el desarrollo de un plan de acción compuesto por programas de seguridad que, una vez implementados, cumplen con los objetivos establecidos. Es importante que la estrategia y los planes de acción incluyan disposiciones para el seguimiento y métricas definidas para evaluar el nivel de éxito. Esto permite realizar ajustes y correcciones en el camino para garantizar que las iniciativas de seguridad estén encaminadas hacia el logro de los objetivos definidos.

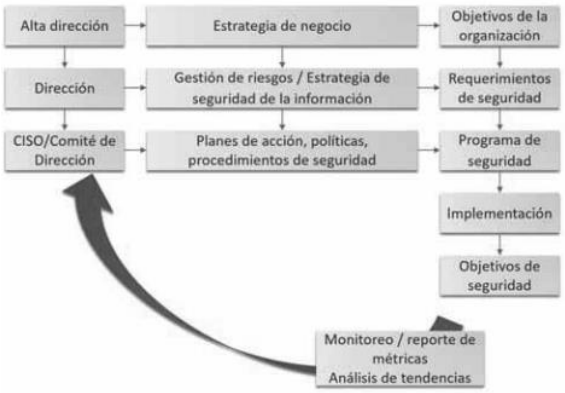

Figura 2 Estrategia alineada a los objetivos

Una vez que los gerentes y directores tienen claridad sobre los

recursos de información necesarios y el nivel de protección requerido, pueden desarrollar e implementar líneas de base de seguridad de la información.

Además, el gobierno de ciberseguridad agrega valor a la empresa al proporcionar una serie de beneficios, tales como mejorar la confianza en las relaciones con los clientes, proteger la reputación de la organización, disminuir la probabilidad de violaciones de privacidad, generar confianza en las interacciones con socios comerciales, permitir nuevas y mejores formas de procesar transacciones electrónicas, y reducir los costos operativos al proporcionar resultados predecibles y mitigar los factores de riesgo que podrían interrumpir los procesos.

En resumen, aunque el gobierno de TI y la ciberseguridad tienen enfoques distintos, son complementarios y necesarios para garantizar la seguridad y eficacia de los sistemas de información. La estrategia de seguridad y el gobierno de ciberseguridad son elementos fundamentales para lograr los objetivos del negocio y brindar beneficios significativos a la empresa.

VIII. GESTIÓN DE ACTIVOS.

En el contexto empresarial, los activos juegan un papel fundamental en la generación de valor y el impulso de las operaciones. Los activos son bienes que posee una empresa y que tienen la capacidad de convertirse en rendimientos económicos, generando futuras entradas de liquidez. Entre los diferentes tipos de activos, se encuentra el activo de información, el cual desempeña un papel crucial en la organización.

Un activo se define como un bien que posee una empresa y que tiene la capacidad de convertirse en dinero u otros medios líquidos. Es esencial que los activos puedan generar rendimientos económicos que se traduzcan en futuras entradas de liquidez para la empresa. Estos activos pueden ser tangibles, como propiedades o equipos, o intangibles, como la propiedad intelectual o los derechos de autor. [1]

Dentro de los activos empresariales, se encuentra el activo de información. Este tipo de activo se refiere a cualquier elemento que tenga valor para la organización y que soporte o sea parte de la actividad, proceso o giro de negocio de la compañía. El activo de información puede incluir datos, sistemas, software, bases de datos, documentos y cualquier otro componente que sea necesario para el funcionamiento y la toma de decisiones de la organización.

El activo de información es crucial para el éxito y la continuidad de una empresa. Dado su valor estratégico, es necesario protegerlo adecuadamente. La protección del activo de información implica implementar medidas y controles de seguridad para salvaguardar la confidencialidad, integridad y disponibilidad de la información. Esto incluye la implementación de políticas de seguridad, el uso de sistemas de protección contra amenazas cibernéticas y la capacitación del personal en buenas prácticas de seguridad de la información.

IX. NORMATIVAS

A continuación, se detallan algunas normativas y estándares relevantes que deben tenerse en cuenta en relación con el dominio de Activos.

Norma ISO27001:2013:

Dentro de esta norma, se encuentran dos puntos clave referentes a los activos:

A.8.1.1. Inventario de Activos: Se establece la necesidad de identificar y elaborar un inventario de los activos asociados con la información y las instalaciones de procesamiento de información. Este inventario debe ser elaborado y mantenido de manera continua [5].

A.8.2.1. Clasificación de la Información: Se establece que la información debe ser clasificada según los requisitos legales, su valor, criticidad y la susceptibilidad a la divulgación o modificación no autorizada. Esta clasificación permite gestionar adecuadamente la protección de la información [5].

Norma ISO27032:

En este estándar se aborda la seguridad de la información en el contexto de las Organizaciones Proveedoras de Información (IPOs). Uno de los puntos relevantes es:

13.2.2 Clasificación y categorización de la información: Se recomienda que las IPOs determinen diferentes categorías de información que recolectan, recopilan, mantienen a salvo y distribuyen. Esta clasificación facilita la implementación de medidas de seguridad adecuadas para proteger la información [6].

Circular externa 007 SFC (Superintendencia Financiera de Colombia):

En caso de que la empresa esté bajo vigilancia de esta entidad, la circular externa 007 SFC establece algunos requisitos específicos:

4.1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y la gestión de identidades. Estos controles deben asegurar que las personas solo tengan acceso a los recursos necesarios para su trabajo durante el tiempo requerido [7].

4.1.2. Adoptar políticas, procedimientos y mecanismos para prevenir la fuga de datos e información. Se deben implementar medidas para evitar la divulgación no autorizada de datos y garantizar la confidencialidad de la información [7].

Estas normativas y estándares son fundamentales para garantizar una adecuada gestión de activos y la protección de la información dentro de las organizaciones. Su cumplimiento contribuye a fortalecer la seguridad de los activos y prevenir riesgos relacionados con la divulgación no autorizada o pérdida de información.

X. CLASIFICACIÓN DE LOS ACTIVOS.

El proceso de clasificación de los activos de información es fundamental para su gestión adecuada. Este proceso implica evaluar el nivel de criticidad de cada activo en relación con los pilares de seguridad: confidencialidad, integridad y disponibilidad de la información. En muchas empresas, se utiliza un enfoque que mide el nivel de cada pilar en tres criterios: alto, medio o bajo, en función del impacto que cada uno de ellos tiene.

Una vez que se ha evaluado el impacto de cada pilar, se realiza un promedio y se asigna una clasificación al activo en función de su nivel de criticidad. Esta clasificación puede ser confidencial, interno o público, dependiendo de los resultados obtenidos.

La figura 3 ilustra de manera gráfica el proceso de clasificación de los activos, mostrando cómo se establecen las categorías en función de la evaluación de los pilares de seguridad.

Figura 3 Clasificación de los activos

El objetivo final de la gestión de activos es darle el tratamiento adecuado a cada uno de ellos según su nivel de criticidad. Esto implica implementar medidas de seguridad y protección acorde a la clasificación asignada, de manera que los activos estén protegidos de forma proporcional a su importancia para la organización.

La clasificación de los activos de información es esencial para establecer prioridades en términos de protección y asignación de recursos. Permite a las organizaciones enfocar sus esfuerzos y recursos en aquellos activos que son más críticos y requieren una atención especial. Asimismo, contribuye a establecer políticas y procedimientos específicos para cada nivel de criticidad, garantizando así un enfoque integral en la gestión de los activos de información y la protección de los mismos.

XI. EVOLUCIÓN DEL GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN.

La evolución del gobierno de seguridad de la información es un proceso constante debido a los avances tecnológicos y a la creciente exposición a riesgos como el robo de identidad, fraude y ataques cibernéticos. Por esta razón, la seguridad de la información se ha convertido en una preocupación a nivel gubernamental en todas las empresas.

Es fundamental comprender que la seguridad de la información es principalmente un problema de gestión que debe abordarse a nivel ejecutivo. A medida que los activos organizacionales se vuelven más intangibles, la protección de la información requiere una atención y recursos mayores. Además, es necesario abordar adecuadamente los requisitos legales y las regulaciones establecidas por los entes de control. Aquellas empresas que no tomen medidas de seguridad adecuadas se exponen a ataques cibernéticos y a la posibilidad de sufrir pérdida de reputación.

Según Aberdeen Group [8], las pérdidas causadas por una seguridad ineficaz se pueden reducir hasta en un 90% mediante la implementación de prácticas de seguridad conocidas y ampliamente utilizadas. Esto demuestra la importancia de una gestión responsable de la seguridad en las empresas.

En la actualidad, las empresas están evolucionando en su enfoque respecto a la seguridad de la información. La alta gerencia está consciente de los riesgos potenciales que pueden materializarse si no logran implementar un gobierno adecuado que controle los activos de información y proteja la confidencialidad, integridad y disponibilidad de los mismos, al tiempo que cumple con las regulaciones correspondientes.

Este cambio de pensamiento y enfoque hacia la seguridad de la información refleja la necesidad de adaptarse a un entorno en constante evolución y de tomar medidas proactivas para garantizar la protección de los activos de información y preservar la confianza de los clientes y socios comerciales. Solo a través de una gestión efectiva y comprometida en seguridad de la información se podrá enfrentar de manera adecuada los desafíos y riesgos asociados con la ciberseguridad en el entorno empresarial actual.

XII. SOLUCIONES DE ESTRATEGIA Y GOBERNANZA.

Para lograr un gobierno adecuado, es necesario identificar soluciones que nos ayuden a llevar a cabo un proceso efectivo. A continuación, se detallan algunas de estas soluciones:

Una estrategia de seguridad sólida es fundamental para establecer los objetivos de seguridad y definir las acciones necesarias para proteger los activos de información. Esta estrategia debe ser alineada con los objetivos y métricas de la empresa, y debe incluir los modelos de seguridad más adecuados según las necesidades específicas.

La evaluación de capacidades y brechas de seguridad permite identificar las fortalezas y debilidades en el entorno de seguridad de la empresa. Mediante esta evaluación, se pueden

identificar las áreas que requieren mejoras y tomar acciones correctivas para cerrar las brechas de seguridad existentes.

El gobierno de datos es esencial para garantizar la integridad, confidencialidad y disponibilidad de la información. Esto implica establecer políticas y procedimientos para la gestión y protección de los datos, así como la asignación de responsabilidades claras para su implementación y cumplimiento.

La resiliencia organizacional y del negocio implica la capacidad de una empresa para resistir y recuperarse de incidentes de seguridad. Esto implica la implementación de medidas de seguridad, respaldo de datos, planes de continuidad del negocio y la capacidad de respuesta efectiva ante incidentes.

El entrenamiento y la cultura son aspectos fundamentales en la estrategia de seguridad. Es importante capacitar a los empleados en prácticas de seguridad y concientizarlos sobre la importancia de proteger la información de la empresa. Fomentar una cultura de seguridad en todos los niveles de la organización ayuda a crear un entorno en el que la seguridad de la información sea una prioridad.

Estas soluciones permiten alinear las prácticas de seguridad con los objetivos empresariales, cumplir con las regulaciones, proteger los datos y garantizar la continuidad del negocio. Al implementar estas soluciones, la empresa podrá identificar los procesos críticos, realizar análisis de impacto de negocio, establecer planes de contingencia y concientizar a su personal sobre la importancia de la seguridad de la información.

XIII. NORMATIVAS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN.

En la implementación y controles para la protección de la información, es fundamental tener en cuenta las leyes y normas establecidas. La figura 4 muestra algunas de estas normas y leyes relevantes en este ámbito.

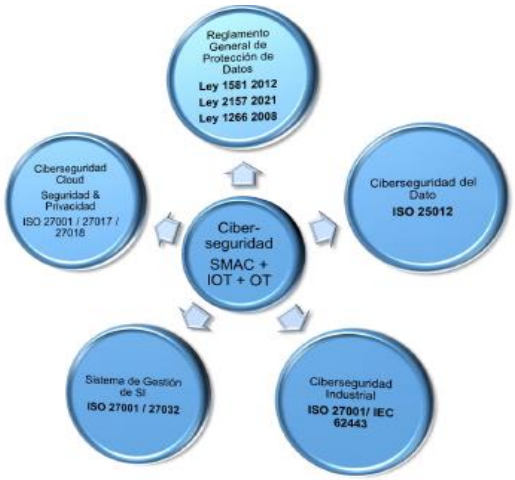

Figura 4 Normas y leyes referente a la protección de la información

Es importante destacar que algunas de estas normas son de estricto cumplimiento, especialmente para aquellas empresas que están bajo la vigilancia y regulación de entes de control específicos. Cumplir con estas normas es un requisito obligatorio para garantizar la protección de la información y evitar posibles sanciones legales.

Además del cumplimiento obligatorio, muchas empresas también adoptan estas normas como buenas prácticas para mejorar su nivel de madurez en cuanto a la seguridad de la información. Implementar estas normas no solo ayuda a proteger los activos de información, sino que también fortalece la confianza de los clientes, proveedores y socios comerciales, y demuestra el compromiso de la empresa con la seguridad y la privacidad de los datos.

Al considerar las leyes y normas relacionadas con la protección de la información, las empresas pueden establecer políticas y controles adecuados, implementar medidas de seguridad eficaces y asegurarse de que sus prácticas cumplan con los estándares requeridos. Esto contribuye a garantizar la integridad, confidencialidad y disponibilidad de la información, y promueve un entorno de confianza tanto interna como externamente.

XIV. CONTROL DE SEGURIDAD.

El control de seguridad desempeña un papel fundamental en la protección de los activos de información de una empresa. Su objetivo principal es asegurar que todos los elementos relacionados con el uso de la Tecnología de la Información, como activos, sistemas, instalaciones, datos y archivos, estén protegidos contra accesos no autorizados, posibles daños y uso indebido o ilegal. Esto implica que estos elementos deben estar operables, seguros y protegidos en todo momento [1].

La implementación de controles de seguridad conlleva numerosos beneficios para la organización. En primer lugar, permite establecer un adecuado gobierno y protección de la información, lo que contribuye a mantener la confidencialidad, integridad y disponibilidad de los datos. Además, los controles de seguridad ayudan a mantener una reputación sólida frente a los clientes, ya que demuestran el compromiso de la empresa con la protección de la información confidencial y la privacidad de los datos.

La disponibilidad de la información es otro beneficio importante de los controles de seguridad. Al establecer medidas de protección adecuadas, se asegura que la información esté disponible cuando sea necesaria para su uso y procesamiento por parte de los usuarios autorizados. Asimismo, los controles de seguridad contribuyen a la protección de los activos de la empresa, evitando pérdidas o daños que podrían surgir como resultado de accesos no autorizados o incidentes de seguridad.

Otro aspecto relevante de los controles de seguridad es su contribución al cumplimiento normativo. Al implementar los controles requeridos por las leyes y regulaciones aplicables, la

empresa puede asegurarse de cumplir con los requisitos legales y evitar posibles sanciones o infracciones. Además, los controles de seguridad permiten gestionar los riesgos de manera controlada, identificando y mitigando las posibles amenazas y vulnerabilidades que podrían afectar la seguridad de la información.

Con esto, podemos decir que, el control de seguridad desempeña un papel esencial en la protección de los activos de información de una empresa. Su implementación proporciona una serie de beneficios, incluyendo un adecuado gobierno y protección de la información, una reputación sólida, disponibilidad de la información, protección de los activos, cumplimiento normativo y gestión controlada de riesgos.

XV. INDICADORES DE SEGURIDAD.

En la actualidad, cada empresa se centra en lograr sus objetivos estratégicos y cumplir con su misión y visión. Para evaluar el desempeño y la madurez del gobierno de seguridad, es necesario llevar a cabo un proceso de medición de la información y un seguimiento constante.

Figura 5 Indicadores de Seguridad

En este sentido, se utilizan indicadores clave de desempeño, también conocidos como KPI (Key Performance Indicators), para reflejar la adquisición de resultados relevantes para la actividad de la empresa. Estos indicadores permiten medir y evaluar el desempeño de los procesos de seguridad de la información y determinar si se están alcanzando los objetivos establecidos.

Por otro lado, se emplean indicadores clave de riesgo, también conocidos como KRI (Key Risk Indicators), para evaluar los riesgos asociados a los ámbitos operacionales de la empresa. Estos indicadores proporcionan advertencias sobre posibles riesgos y permiten anticipar problemas y oportunidades futuras. Se basan en la observación de tendencias y patrones que podrían afectar a la organización en términos de seguridad de la información.

Mientras que los KPI se centran en datos históricos y en la medición del desempeño pasado, los KRI se enfocan en el pronóstico de lo que podría suceder en el futuro. Ayudan a identificar y prever posibles riesgos y situaciones que podrían afectar a la organización, lo que permite tomar acciones preventivas y mitigar los impactos negativos.

Por lo tanto, los indicadores de seguridad, tanto los KPI como los KRI, son herramientas importantes para evaluar el desempeño y los riesgos relacionados con la seguridad de la información en una organización. Estos indicadores permiten medir y evaluar el rendimiento pasado y anticipar posibles problemas futuros, lo que facilita la toma de decisiones informadas y la implementación de medidas preventivas y correctivas adecuadas.

XVI. ¿QUÉ ES UNA COMUNIDAD DIGITAL?

Las comunidades digitales o virtuales son agrupaciones de personas reales que se forman en plataformas en línea, como redes sociales o espacios de encuentro, con el propósito de intercambiar información, tanto formal como informal. Estas comunidades reúnen a individuos que comparten intereses en común y buscan establecer lazos y relaciones a través del aprendizaje comunitario.

Al igual que las comunidades tradicionales, las comunidades digitales se basan en la interacción entre sus miembros y en el intercambio de conocimientos y experiencias. Sin embargo, a diferencia de las comunidades físicas, los encuentros en las comunidades digitales se llevan a cabo de manera virtual, a través de plataformas y herramientas digitales.

En la consolidación de una comunidad digital, el flujo constante de información juega un papel fundamental. Los miembros comparten contenido, realizan discusiones, plantean preguntas y brindan respuestas, lo que fortalece los lazos y fomenta el aprendizaje colectivo [9].

Sin embargo, las comunidades digitales también enfrentan desafíos. En la figura 6 se presentan algunos de estos desafíos, que incluyen la gestión de la privacidad y la seguridad de la información, la moderación de los contenidos, la participación activa de los miembros y la creación de un ambiente inclusivo y respetuoso.

Figura 6 Desafíos de Comunidades Digitales

En este sentido, las comunidades digitales son espacios virtuales donde las personas se agrupan para intercambiar información, aprender y establecer relaciones basadas en intereses comunes. Estas comunidades se apoyan en el flujo constante de información y enfrentan desafíos relacionados con la gestión y la participación activa de los miembros.

XVII. IMPORTANCIA DE LAS COMUNIDADES DIGITALES.

La importancia de las comunidades digitales radica en su capacidad para fomentar la colaboración y el aprendizaje grupal, lo que a su vez impulsa el desarrollo de nuevos conceptos, proyectos o productos. Estas comunidades permiten establecer redes de interacción y comunicación en línea, lo cual es fundamental para la gestión del conocimiento, ya que amplía la diversidad de perspectivas y enriquece la red de la comunidad.

Un ejemplo claro de la relevancia de las comunidades digitales se ha dado durante la pandemia de COVID-19. En este contexto, estas comunidades han experimentado un crecimiento significativo al utilizar herramientas digitales para el intercambio de información, generando nuevos espacios de colaboración y aprendizaje que antes no tenían un valor tan significativo.

En la actualidad, estas comunidades en línea se utilizan de manera constante tanto en el ámbito laboral como educativo. Se han convertido en espacios donde se transmite conocimiento en diferentes procesos y áreas temáticas, adaptándose al alcance y las necesidades de cada comunidad específica.

No obstante, uno de los desafíos más importantes que se deben abordar en estas comunidades es el tema de la regulación y el comportamiento de los usuarios. Como se menciona en el refrán "Una manzana podrida puede estropear el barril"[10], es necesario establecer normas y reglamentos para evitar el mal comportamiento dentro de la comunidad. Esto implica garantizar el cumplimiento de las leyes, como la Ley de Protección de Datos Personales 1581 de 2012, y asegurarse de que las normas promuevan el crecimiento y fortalecimiento de la comunidad en lugar de convertirla en un espacio de burla, ciberacoso o difusión de noticias falsas. De esta manera, se protege la reputación de la comunidad frente a la organización y se fomenta un ambiente respetuoso y constructivo.

XVIII. TIPOS DE COMUNIDADES DIGITALES

En el estudio realizado por Jonassen, Peck y Wilson en 1999 se identificaron cuatro tipos de comunidades digitales que se pueden encontrar en el contexto actual:

Figura 7 Tipos de comunidades Digitales.

Cada tipo de comunidad digital tiene su propia dinámica y propósito, pero todas ellas comparten el objetivo de conectar a individuos con intereses comunes y facilitar la interacción, el aprendizaje y el apoyo mutuo en el entorno digital.

XIX. EL GOBIERNO DE TI Y SU IMPACTO EN LAS COMUNIDADES DIGITALES

El gobierno de TI desempeña un papel fundamental en el impacto y la gestión de las comunidades digitales. A continuación, se presentan diferentes aspectos en los que el gobierno de TI puede influir y contribuir al desarrollo y funcionamiento de estas comunidades.

En primer lugar, la participación de los usuarios es un aspecto clave en las comunidades digitales. El gobierno de TI puede facilitar la participación activa de los usuarios al proporcionar plataformas y herramientas digitales que promuevan la toma de decisiones colaborativa y la expresión de ideas y opiniones. Esto fortalece la democracia digital y fomenta la inclusión, al brindar a todos los usuarios la oportunidad de ser escuchados.

Además, el gobierno de TI tiene la responsabilidad de proteger los derechos digitales de los usuarios en las comunidades en línea. Esto implica garantizar la confidencialidad de los datos, salvaguardar la libertad de expresión y promover el acceso equitativo a la información. A través de procesos de estandarización adecuados y el cumplimiento de las leyes pertinentes, se puede proporcionar un entorno digital confiable y seguro.

Otro aspecto importante es la promoción de la igualdad y la diversidad en las comunidades digitales. El gobierno de TI puede desempeñar un papel clave en la implementación de políticas inclusivas y programas de capacitación que busquen cerrar la brecha digital y garantizar la participación igualitaria de todos los usuarios en los espacios digitales, sin importar su género, raza, edad o ubicación geográfica.

Asimismo, el gobierno de TI debe abordar la regulación de la desinformación y el discurso de odio en las comunidades en línea. Esto implica establecer regulaciones claras y efectivas para prevenir la propagación de información falsa y garantizar que el entorno digital sea seguro y confiable para todos los usuarios.

Finalmente, el gobierno de TI debe fomentar la colaboración entre el sector público, el sector privado y la sociedad civil para abordar los desafíos y aprovechar las oportunidades que surgen en las comunidades digitales. Esta colaboración puede incluir la formación de alianzas estratégicas, la participación en diálogos y la ejecución conjunta de políticas y proyectos relacionados con las comunidades en línea.

XX. DESAFIOS Y CONSIDERACIONES

El gobierno de TI se enfrenta a una serie de desafíos y consideraciones en relación con las comunidades digitales. A continuación, se presentan algunos de los desafíos más importantes que deben abordarse:

En primer lugar, la protección de la privacidad es un desafío clave. El gobierno de TI debe encontrar un equilibrio entre la protección de la privacidad de los usuarios y la necesidad de recopilar datos para mejorar los servicios y garantizar la seguridad en las comunidades digitales. Es necesario establecer políticas y regulaciones que protejan los datos personales de los usuarios y al mismo tiempo permitan un uso adecuado de la información.

El segundo desafío está relacionado con la velocidad del cambio tecnológico. Las comunidades digitales evolucionan rápidamente y las tecnologías subyacentes están en constante desarrollo. Esto plantea un desafío para el gobierno de TI, ya que debe mantenerse actualizado y adaptarse a los cambios para garantizar una regulación efectiva y una protección adecuada de los usuarios. Es importante revisar y actualizar regularmente las leyes y políticas existentes para que sean pertinentes y adecuadas a las nuevas circunstancias.

Otro desafío importante es el equilibrio entre la censura y la libertad de expresión. El gobierno de TI debe encontrar una forma de regular el contenido en las comunidades digitales para evitar la difusión de contenidos dañinos o ilegales, como el discurso de odio o la desinformación. Sin embargo, también es fundamental proteger la libertad de expresión y evitar la censura injustificada. Esto requiere un enfoque equilibrado que permita la expresión libre y segura de ideas sin poner en peligro la seguridad y el bienestar de los usuarios.

Abordar estos desafíos de manera efectiva es esencial para garantizar un entorno digital seguro, proteger los derechos de los usuarios y promover el desarrollo saludable de las comunidades digitales.

IX. CONCLUSIÓNES

En conclusión, el gobierno de TI desempeña un papel crucial en la ciberseguridad y debe integrarla como parte integral de sus políticas y prácticas. Esto implica contar con el apoyo de la alta gerencia para garantizar la confidencialidad, integridad y disponibilidad de la información. Establecer métricas como los KPI o KRI desde el gobierno de TI y ciberseguridad permite tomar decisiones basadas en resultados concretos.

Es fundamental que toda comunidad, sin importar su temario, cuente con procesos de TI y ciberseguridad para proteger la información transmitida en el grupo. Esto implica implementar políticas y prácticas que salvaguarden la confidencialidad de los datos y prevengan accesos no autorizados. La concientización juega un papel clave en la seguridad de la información de las empresas, por lo que se debe implementar un plan de trabajo sólido para capacitar a los empleados sobre la importancia de la seguridad y los beneficios que conlleva.

Los desafíos que enfrentan las comunidades digitales también son determinantes para su éxito. Estos desafíos incluyen la protección de la privacidad, la gestión del cambio tecnológico, la regulación del contenido, la lucha contra la desinformación y la promoción de la igualdad y la diversidad. Abordar estos desafíos de manera efectiva es esencial para crear y gestionar comunidades digitales exitosas.

En última instancia, la creación y gestión de comunidades digitales ofrece numerosos beneficios, como el acceso a la información, la participación y colaboración entre sus miembros. Estas comunidades fomentan actividades basadas en la comunicación, análisis y reflexión, lo que promueve un entorno propicio para el intercambio de conocimientos y experiencias. En conjunto, el gobierno de TI, la ciberseguridad y el enfoque en los desafíos y consideraciones específicos permiten desarrollar y mantener comunidades digitales sólidas y exitosas.

RECONOCIMIENTO

Agradezco a la Universidad Piloto de Colombia que a través de las clases de la especialización de seguridad informática y del coterminal “maestría en Seguridad Informática y de las Comunicaciones”, logre adquirir y reforzar conocimientos importantes de seguridad informática y ciberseguridad especialmente el tema enfocado a Gobierno y Comunidades Digitales. Este conocimiento que he adquirido gracias a la metodología de los docentes y las herramientas brindadas me han ayudado a entender la importancia que debemos tener hoy en día este proceso y poder colocarlo en práctica tanto en la vida profesional como laboral.

REFERENCIAS

[1] Docente. Lorena Ocampo Presentación de la materia “Gobierno TI” del coterminal maestría en Seguridad Informática y de las Comunicaciones – Universidad Piloto de Colombia. [2023]
[2] Cobit 4.1, IT Governance Institute. www.itgi.org [2007].
[3] IT Governance Institute "Information Security Governance Guidance for Boards of Directors and Executive Management", 2nd Edition. [2006]
[4] Palao, M. . Reflexión sobre el Estado del Arte del Buen Gobierno TIC. Bogotá:ISACA [2010]
[5] ISO27001 Sistema gestión de seguridad de la información [2013]

[6] ISO27032 Directrices para la ciberseguridad [2012]
[7] Circular externa de la SFC 007 Requerimientos Mínimos Para La Gestión De La Seguridad De La Información Y La Ciberseguridad [2018]
[8] Aberdeen Group, "Best Practices in Security Governance", USA, [2005]
[9] Docente. Fabian Gaitan Presentación de la materia "Seminario de tecnología ciencia y sociedad" [2023] del coterminal maestría en Seguridad Informática y de las Comunicaciones – Universidad Piloto de Colombia. [2023]
[10] Building successful online communities: Evidence-based social design. Cambridge, Mass: MIT Press. Kraut, R. E., Resnick, P., & Kiesler, S. [2011].

AUTOR:

Andres R. Cuervo F. Nació en Bogotá, Colombia en 1990. Ingeniero de sistemas, Egresado de la Escuela Tecnológica Instituto Técnico Central la Salle en el año 2017, Bogotá-Colombia, me he desempeñado en distintos roles relacionados en el área de Seguridad de la Información y Riesgos, cuento con la certificación de auditor interno ISO 27001:2013 e ISO 22301:2019, Adicionalmente cuento con un Diplomado referente a seguridad de la información realizado en la EUD y Cursos cortos referente a ciberseguridad ISO 27032 y Seguridad en la nube. Actualmente realizando la especialización en seguridad informática en la Universidad Piloto de Colombia.