Importancia de estructurar un Gobierno de Seguridad y Ciberseguridad en las organizaciones.
(Noviembre 2022)

Holber Hernández
Especialización en Seguridad Informática
Holber-Hernandez@upc.edu.co

Abstract— Organizations must understand that the definition of a cybersecurity government allows them to improve their organizational processes, define lines of defense and scope that give added value to information assurance. In addition, it helps senior management to be an integral part of the process, helping to permeate the entire organization, not only thinking about the cost and return on investment and defining the guidelines, but also being the internal factor that generates support. of the Cybersecurity and security government, giving reliability to its clients by applying good technological assurance practices, in order to avoid incurring errors and sanctions for non-compliance that may affect their reputation.

The document is made up of the following line topics, a risk assessment with its current status, the definition of guidelines and policies, awareness, and measurement to apply defense to continuous improvement. These factors are the ones that must be taken into account by the organization when creating or improving its security and cybersecurity governance, therefore, reaching out to all those involved, relying on technical frameworks and good practices, developing good governance management. of the defined government, to condense and gain strength in organizations with the new technological changes and the constant risk in which information is found, where the Cybersecurity and Technology Security areas must be in constant work to prevent these risks from affecting the organization and are controlled and monitored**.**

Keywords— Cybersecurity, risk, threats, lines of defense, policies, assurance guidelines, measurement, governance and awareness.

***Resumen*— Las organizaciones deben entender que la definición de un gobierno de ciberseguridad les permite mejorar sus procesos organizacionales, definir líneas de defensa y alcances que den valor agregado al aseguramiento de la información. Además, que ayuda a la alta dirección para que sean parte integral del proceso apoyando a permear a toda la organización, no solo pensar en el costo y retorno de la inversión y definir los lineamientos, si no en ser el factor interno que genera el respaldo del gobierno de Ciberseguridad y seguridad dando la confiabilidad ante sus clientes aplicando buenas prácticas de aseguramiento tecnológico, con el fin de evitar incurrir en errores y sanciones por incumplimiento que puedan afectar su reputación.

El documento está compuesto por los siguientes temas líneas de defensa, una evaluación de riesgo con su estado actual, la definición de lineamientos y políticas, concienciación y la medición para aplicar la mejora continua. Estos factores son los que deben tenerse en cuenta por la organización en el momento de crear o mejorar su gobierno de seguridad y ciberseguridad , por consiguiente, dar alcance a todos los involucrados apoyándose en los marcos técnicos y buenas prácticas generando una buena gestión de la gobernanza del gobierno definido, para condensar y tomar fuerza en las organizaciones con los nuevos cambios tecnológicos y el constante riesgo en que se encuentra la información, en donde las áreas de Seguridad Ciberseguridad y Tecnología deben estar en constante trabajo para evitar que estos riesgos afecten a la organización y sean controlados y monitoreados.

***Palabras Clave*— Ciberseguridad, riesgo, amenazas, líneas de defensa, políticas, lineamientos, aseguramiento, medición, gobernanza y concienciación.**

I. INTRODUCCION

Uno de los hitos de gran importancia en las empresas es la seguridad informática y Ciberseguridad, ésta debe ir alineada con los avances tecnológicos, por el crecimiento de los delitos y ataques informáticos, los cuales están impactando las organizaciones generando daños irreparables es por esto que se debe replantear definiendo los gobiernos de Seguridad y Ciberseguridad.

El proceso de implementar los gobiernos de ciberseguridad es poder definir sus líneas de defensa con las que debe contar la organización para distribuir jerarquía y atacar cada uno de los problemas y procesos que conforman el gobierno de seguridad. Por otro lado, tenemos lo que es el estado actual de la organización frente a las posturas de seguridad y ciberseguridad por medio de los análisis de riesgo organizacional para identificar esas amenazas que pueden comprometer los sistemas de información.

También se debe tener presente la definición de las políticas y lineamientos que son estructuradas en el gobierno de seguridad a nivel de procedimientos para garantizar el uso de las buenas prácticas de seguridad que nos dan algunos marcos como lo son COBIT5, ITIL, NIST 800-32 y 27001 con el fin de adoptar lo que se ajusta a las necesidades y moldear con la organización. De aquí se permite dar partida al tema de concienciación, en donde se debe dar a conocer y generar planes de concienciación para entrenar y capacitar los funcionarios, desarrollando capacidad de respuesta teniendo en cuenta cada uno de los lineamientos y políticas que deben cumplir ayudando a ser parte del proceso. Por medio de la gobernanza y apoyo de los altos directivos se logra permear a toda la organización y dar alcance a todos lo proceso de negocio que deben conocer de primera mano cómo se encuentra conformado el gobierno de seguridad y ciberseguridad.

El desarrollo de los procesos mencionados anteriormente se identifica medir toda la gestión y medidas procesos que se implementaron, por medio de KPI, KRI y a nivel de negocio el Balance Scorecare, para aplicar la mejora continua y saber el nivel de desempeño del gobierno de seguridad en cuanto al negocio y la organización.

II. LÍNEAS DE DEFENSA

Las líneas de defensa cubren las funciones de aseguramiento, gobierno, riesgo, cumplimiento, seguridad de la información y ciberseguridad según ISACA [1] permitiendo a las organizaciones establecer el gobierno de ciberseguridad que pueden moldear la estrategia de negocio y de esta manera apuntar a sus objetivos organizacionales.

A continuación, se describe en la Ilustración 1 cada una de las líneas de defensa que deben definirse en el gobierno de Ciberseguridad desde la línea jerárquica:

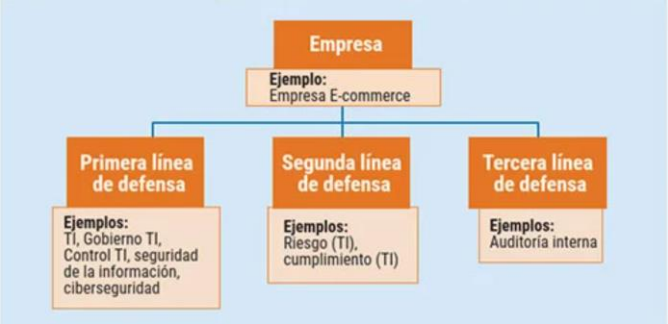

Ilustración 1Ejemplo de estructurar Líneas de defesa, ISACA. [1]

Con base en lo propuesto por ISACA se argumentará cada una de las líneas de defensa:

A. Primera línea-Aseguramiento: aquí encontramos las áreas que hacen parte de la estructura organizacional de acuerdo al tamaño o nivel de madurez de la compañía estos pueden variar, por lo general están las áreas de tecnología, en donde tenemos Ciberseguridad o TI quienes son los encargado del aseguramiento de la infraestructura tecnológica y su operación por medio de inclusión, diseño y gestión de los controles de seguridad tecnológica en la organización y son los primeros en actuar ante un incidente o evento de seguridad que pueda presentarse. De acuerdo con la estructura definida la primera línea es el insumo para la segunda línea de defensa de continuidad a procesos y temas de más alto nivel.

B. Segunda Línea - Riesgos y Cumplimiento: Esta es considerada la línea de apoyo, en donde se encuentra definida las directrices y políticas de seguridad de la información que deben cumplirse al interior de las organizaciones, generalmente es liderada por los equipos de seguridad de la información y son quienes dan estricto cumplimiento a los temas normativos que exigen los entes reguladores desde la definición de sus lineamientos. Otro papel que es de gran valor y se considera la columna vertebral es el proceso de análisis de riesgo de la organización, el cual es trabajado de la mano con la primera línea de defensa en el seguimiento continuo de las amenazas que puedan presentarse.

C. Tercera Línea - Auditoria: Esta es la línea que permite que la organización cuente con la mejora continua, mediante los procesos de auditoría, en donde se evalúa lo definido por la segunda línea y los proceso que se ejecutan en la primera línea para detectar errores o incumplimientos que deben ejercer planes de acción. Además, que hace parte del proceso de control interno de la organización y dar un parte o estatus a la alta dirección del estado actual del gobierno de Seguridad.

III. Estado Actual-Evaluación De Riesgo Cibernético

El análisis actual es fundamental para identificar el estado en que se encuentra la organización, es por esto que se debe definir una evaluación de riesgos cibernéticos para comprender las brechas y crear una hoja de ruta para cerrar las amenazas que pueden Identificarse en la organización.

A. Evaluación de Riesgo de Ciberseguridad y Seguridad de la Información.

Para definir un análisis de riesgo cibernético debemos empezar a evaluar los activos que se encuentran involucrados, una vez identificados, se debe validar que amenazas potenciales tenemos que trabajar para empezar a generar los planes de acción y aplicar controles correspondientes.

Uno de los marcos de referencia más usados para todo tipo de organización es el NIST framework Cybersecurity [2], El cual está diseñado para la gestión de los riesgos cibernéticos por medio de sus cinco funciones o etapas:

- **Identificar:** Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de: sistemas, activos, datos y capacidades [3].
- **Proteger:** Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios [3].
- **Detectar:** Desarrollar e implementar las actividades apropiadas para identificar cuando ocurra un evento de ciberseguridad [3].
- **Responder:** Desarrollar e implementar las actividades apropiadas para tomar acción en relación con un evento de ciberseguridad detectado [3].
- **Recuperar:** Desarrollar e implementar las actividades apropiadas para mantener planes para la resiliencia y para reestablecer cualesquiera capacidades o servicios que hayan sido afectados durante un evento de ciberseguridad [3].

A continuación, encontramos en la ilustración 2 las cinco funciones o etapas definidas por NIST que se detallaron anteriormente, visualizadas a continuación:

Ilustración 2 Cybersecurity Framework V1.1 [3]

Con base en la ilustración 2 podemos identificar las cinco funciones del marco de Ciberseguridad que fueron descritas anteriormente, en este caso el foco está en la primera función que es "**IDENTIFY**" donde se componen dos categorías importantes que son "**Risk Assesment**" y el "**Risk Management Stategy**" en el cual se detallan las subcategorías y la información de referencia para aplicar referente a riesgos y tener una base de establecer el estado actual de la organización como lo observamos en la ilustración 3:

ID.RA-1: Asset vulnerabilities are identified and documented	· **CCS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
ID.RA-3: Threats, both internal and external, are identified and documented	· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
ID.RA-4: Potential business impacts and likelihoods are identified	· **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
ID.RA-6: Risk responses are identified and prioritized	· **COBIT 5** APO12.05, APO13.02 · **NIST SP 800-53 Rev. 4** PM-4, PM-9
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	· **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **NIST SP 800-53 Rev. 4** PM-9
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **NIST SP 800-53 Rev. 4** PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14

Ilustración 3 Subcategorías de Risk ID.RA-ID.RM [2]

Además, como observamos en la ilustración 3 este marco también hace referencia a otros estándares como lo son COBIT5, ISA, CCS, ISO 27001:2013 y la propia NIST referenciando los controles y mediadas recomendadas para trabajar los temas de riesgo de ciberseguridad dentro de las organizaciones. Es importante que las organizaciones incluyan este marco de referencia al interior el cual es público y no tiene costos adicionales y se acomodan a las necesidades y tipos de organizaciones.

B. Evaluación de madurez de Ciberseguridad y Seguridad de la Información.

El assesment de madurez en las organizaciones es un punto crucial para dar un paso adelante siempre y cuando se tiene definido el estado actual y se ha identificado un punto de balance según los objetivos de negocio de la organización, uno de los elementos importantes es el proceso de mejora continua que se ha definido y permite definir métricas que a su vez ayudan a los directivos de la alta dirección quienes conforman el gobierno de ciberseguridad y seguridad de la información a actuar y generar alertas según sus apetitos de riesgo.

La madurez es el estado o nivel que se basa en supuestos que definen las organizaciones frente a su estado de tranquilidad. Estos son esfuerzos permanentes de los lideres que retan las prácticas de forma permanente sacando al sistema de la zona de confort y generan condiciones diferentes cada vez para conformar una perspectiva nueva de la experiencia de seguridad y control [4].

Los gobiernos de Ciberseguridad y Seguridad de la información deben definir sus apetitos de riesgo frente a sus análisis de riesgo organizacionales, con el fin de aplicar cada vez más con sus equipos de trabajo, el aseguramiento a profundidad o también conocido como seguridad en capas creando barreras de protección a los activos de información y permiten que las herramientas entren en un estado de madurez que ya su foco no es solo operarlas sino cambiar el alcance de garantizar que se puedan explotar todas sus funcionalidades y puedan llegar a el 100% de las herramientas de seguridad.

Un ejemplo de definición de apetitos de riesgo que nos menciona MinTIC son los que se identifican en la Ilustración 4:

Ilustración 4 Eje. Modelos madurez según MinTIC [5]

De acuerdo con la Ilustración 4, que MinTIC plantea son los niveles de madurez que busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en las organizaciones [5].

Es cierto que la tecnología siempre va a tener cambios y está en constante actualización lo cual nos obliga a estar evaluando los apetitos de riesgo y los niveles, los cuales puede llegar a cada organización siempre alineados a sus procesos core y temas de negocio.

C. Estructura organizacional del gobierno de seguridad y Ciberseguridad.

La estructura organizacional del gobierno de Ciberseguridad y Seguridad debe estar clara y definida en un organigrama, identificando sus niveles jerárquicos correspondientes, para definir responsabilidades y tomas de decisión, es por ello que la alta dirección y las áreas de negocio correspondientes estén en el proceso ya que las disposiciones que se tomen pueden impactar de manera transversal a la organización y de esta forma tener una buena gobernanza por la parte Directiva y el CISO.

La estructura del gobierno puede ser definida por decisión propia bajo el modelo que escoja la organización, pero mínimo debe contar con:

- Alta Dirección.
- Directivos.
- CISO.
- Responsables o líder de cada una de las líneas de defensa que defina o adopte la organización.

La definición o conformación del gobierno, debe quedar plasmado y documentado con la matriz de responsabilidades de cada uno de los encargados.

Algunas de las responsabilidades que debe asumir la alta dirección o Junta Directiva es la supervisión estratégica a la seguridad de la información e incluir [6]:

- Entender la criticidad de la información y su seguridad para la organización [6].
- Revisar y evaluar la inversión en ciberseguridad y seguridad de la información, alineada con la estrategia y los perfiles de riesgo [6].
- Respaldar los desarrollos de los programas de Ciberseguridad y seguridad de la información [6].
- Exigir reportes o informes de manera periódica sobre la adecuación de los programas y eficiencia de estos [6].

Lo mencionado anteriormente genera valor al gobierno de seguridad y ciberseguridad al interior permitiendo tener una buena gobernanza según lo dice Governance Institute en su libro Information Security Governance [6], en donde podemos identificar:

- Mejorar y proporcionar confianza en las relaciones con los clientes y socios.
- Proteger la reputación de la organización.
- Disminuir la probabilidad de ataques que afecten la privacidad de la información.

- Permitir nuevas formas de negocio que ayudan con el aseguramiento en el procesamiento de transacciones.
- Reducir costos operativos obteniendo con resultados predecibles de la mitigación de riesgos que se evaluaron en la organización.
- Generación de alertas tempranas para actuar ante determinadas situaciones de amenaza.

Otro factor importante de la estructura organizacional es contar con capacidades de recursos humano para cada uno de los procesos y no se tengan solo definidos a nivel documental, como ocurre en muchas organizaciones, en donde se logra plasmar una buena estructura de gobierno y un diseño adecuado, pero la organización o no cuenta con los recursos o no tiene su planta completa para dar alcance a lo definido y tenemos profesionales en donde cubren todos estos vacíos y se cometen errores que pueden impactar el negocio. Por esta razón se debe contar con los recursos correspondientes tanto humano, de herramientas, capacitación y transferencias de conocimiento al interior.

Con esto podemos cerrar este punto diciendo que es de valor que las organizaciones puedan definir una hoja de ruta alineada al negocio y una estructura del gobierno de seguridad y ciberseguridad para cumplir sus objetivos a cabalidad.

IV. Definición de Lineamientos y Políticas.

Los lineamientos y políticas son el soporte de todo el gobierno de Ciberseguridad y seguridad de la información permitiendo definir sus objetivos, alcances, responsabilidades, para la gobernanza y con esto poder abarcar a toda la organización.

La definición de las políticas y lineamientos del gobierno de seguridad y Ciberseguridad según los estándares marcos de referencia o normas técnicas como son:

- ISO/IEC 27001:2013 SGSI
- ITILV4 - Modelo de Gobierno
- COBIT5 - Marco de trabajo TI
- NIST SP 800-53 - Marco de Ciberseguridad
- CCS – CIS Center for Internet Security

Con los marcos de referencia mencionados anteriormente la organización está en la capacidad de tomar o adoptar el que mejor se acomode a sus necesidades y no precisamente tienen que cumplirlo o acoger a cabalidad, sino sirven como base para aplicar las metodologías que ayudan a que se puedan construir con el apoyo del CISO y la alta dirección, como resultado definiendo los lineamientos y políticas que enmarcan a el gobierno y a su vez a los objetivos estratégicos de la organización. Por tal motivo no todos los gobiernos son iguales ya que el foco de negocio no es el mismo, así se tenga la misma línea acción en diferentes organizaciones, debido a que las estructuras organizaciones son completamente diferentes al igual que los objetivos y recursos. Por lo tanto, los lineamientos y políticas van a ser diferentes.

Para empezar a definir lo que es un lineamiento y una política vamos a dar las siguientes definiciones:

- **Política**: Según la ISO 27000 una política define como el compromiso general, dirección o intensión. Esto expresa el compromiso formal de administración para implementar y mejorar un SGSI [7]. Enfocado al gobierno son esas buenas prácticas adoptadas por la organización para dar cumplimiento al objetivo de negocio junto al gobierno de Ciberseguridad y seguridad.

- **Lineamiento**: Según la RAE hace referencia a rasgo característico de algo [8]. Enfocándolo a el gobierno de seguridad se puede hacer referencia a la especificidad y estricto cumplimiento de una política de seguridad.

Con base en las definiciones anteriores podemos argumentar que son complementarias una de la otra para el Gobierno de Ciberseguridad, en sus políticas a un alto nivel. Si nos enmarcamos en lo que menciona el estándar de COBIT5, en donde tiene en cuenta los siguientes objetivos, para definir las políticas del gobierno [9]:

- Asegurar un buen gobierno, protegiendo los interese de los skateholders (Clientes, accionistas, empleados, etc.) [9] definido en las políticas de la organización.
- Garantizar el cumplimiento normativo del sector al que pertenezca la organización [9] con base a las directrices de los entes reguladores.
- Mejorar la eficacia y eficiencia de los procesos y actividades de la organización [9], como parte del proceso de mejora continua.
- Garantizar la confidencialidad, integridad y disponibilidad de la información [9]. De acuerdo con la política de seguridad de la información.

Por consiguiente, tenemos al IT Governance Institute quien da las pautas para lograr un gobierno de Seguridad y Ciberseguridad [6] que permita adoptar las políticas a la buena gobernanza y a su vez garantizar un nivel al que debe llegar a la organización haciendo uso de las buenas practica bajo esos lineamientos que fueron estructurados al interior.

Una vez se han definido las políticas de seguridad, deben garantizar su socialización y publicación para los skateholders de la organización, tanto nivel interno y externo para dar y socializar los lineamientos correspondientes y exigir su cumplimiento.

De acuerdo con la ISO 27001:2013 en su Clausula 5.2 nos habla sobre las políticas y hace referencia a la alta dirección como parte fundamental en la definición de las políticas específicamente lo siguiente [10]:

La alta dirección debe establecer una política de seguridad de la información que cumpla con lo siguiente [10]:

- Sea adecuada al propósito de la organización
- Incluya objetivos de seguridad de la información y proporcione marcos de referencia.
- Incluya los compromisos de cumplir los requisitos aplicables relacionados con la seguridad de la información.

La política de seguridad de la información debe [10]:

- Estar disponible como información documentada.
- Comunicarse y socializarse dentro de la organización.
- Estar disponible para consulta según su nivel y asegurando que es el propietario.

Como observamos va muy alineada al marco COBIT5 con enfoques diferentes pero el Mismo objetivo que garantizar el propósito de la organización las partes interesadas y la triada (confidencialidad, integridad y disponibilidad) de Seguridad de la información.

Hay que recordar que para llegar a tener el nivel de madurez de un gobierno de seguridad se debe contar con un muy buenas definiciones y alineaciones a los objetivos de negocios de las políticas de Seguridad y Ciberseguridad dentro de la organización y esta es una de las primeras bases con las que se debe tener una sólida construcción, para empezar a impartir la buena gobernanza de gobierno de ciberseguridad y seguridad de la información.

V. AWARENESS DE CIBERSEGURIDAD

Uno de los puntos clave para llegar al proceso de madurez que todo gobierno de ciberseguridad y seguridad debe cumplir es el tema de concienciación, también conocido como awareness, en donde parte del apoyo de toda la organización y permite permear a todos los skateholders.

Es de conocimiento que el eslabón más débil sigue siendo el usuario final o el funcionario (las personas). Esto se debe a la falta de desconocimiento y falta de capacitación hacia los funcionarios de la organización y es fundamental educar a los empleados en las buenas prácticas de seguridad y ciberseguridad del mundo digital actual.

La capacidad de una organización para hacer frente a las amenazas y vulnerabilidades de la actualidad depende en gran medida de los niveles de formación y concienciación en ciberseguridad del personal, en consecuencia, de la existencia de un marco de competencias que identifique los contenidos y niveles de formación y concienciación necesarios para cada puesto de trabajo [11] sin excepción algún para dar alcance a un nivel de detalle más específico.

Por otro lado según la revista Pixel Bit en el artículo de Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura [12], dice que la ciberseguridad se ha convertido en una de las áreas de las TIC que mayor atención y esfuerzo ha recibido en los últimos años, debido tanto a la necesidad de dar respuesta al constante crecimiento y sofisticación de los ataques y riesgos a los que se enfréntala sociedad, como al desarrollo incesante de la propia tecnología. En este entorno, en el que el factor humano es un aspecto crucial, las actividades de formación y concienciación en ciberseguridad son elementos críticos, en los que se debe profundizar, actualizar y mejorar de manera constante.

Lo descrito anteriormente es muy cierto a lo que se está presentando hoy día las nuevas amenazas y vulnerabilidades hacen que debamos estar en constante aprendizaje, si para los profesionales de TI y ciberseguridad es un reto aún más lo es para los funcionarios que no son de las áreas de TI que es por donde se logra generar esas puertas traseras.

La importancia del apoyo de la alta dirección es fundamental en las organizaciones por consiguiente de ahí parten los lineamientos que ayudaran a difundir y estar en contante aprendizaje de como:

- Actuar
- Reportar
- Bloquear
- Disuadir

Todos los tipos de ataques que puedan llegar a materializarse en las organizaciones y trabajar en el proceso de contención, en lo que respecta hay muchos de estos efectivamente van a lograr materializarse. Por lo tanto, en el proceso de madurez de los gobiernos de seguridad se cuenta con un sólido conocimiento y plan de concienciación, cuando es liderado por el CISO al poder dar alcance a todos los funcionarios.

Las amenazas y tipos de ataques a los cuales están expuestas las organizaciones son de gran variedad y diversidad. A continuación, se exponen algunos que ya son conocidos por las áreas de ciberseguridad y según ISACA [13] se definen de la siguiente manera:

- **Ransomware**: Software que infecta equipos y realiza cifrado de la información evitando el acceso a los usuarios legítimos y solicita un pago para su rescate.
- **Spyware**: Software espía que captura y trasmite la información de navegación, contraseñas, tarjetas de crédito, etc. a un equipo central que es controlado por el atacante.

- **Keylogger**: Captura de pulsaciones del teclado y guarda información en un archivo local que es actualizado y enviado al atacante.
- **Rootkit**: Tiene la capacidad de manipular el sistema operativo para ocultarse los usuarios legítimos. No sale en los procesos ni directorios que se listen.
- **Botnet**: Redes de PCs infectados y de manera coordinada hace tareas definidas por un atacante.
- **Virus**: Software malicioso capaz de reproducirse en otros dispositivos.
- **Drive-by download**: Archivos que pueden dañar equipos móviles.
- Gusano: Software que se propaga por medio de la red y sobrecarga las computadoras conveniencia del atacante.
- **Troyano**: Archivos ocultos dentro de un archivo legítimo que, en su ejecución, activa el archivo malicioso.
- **Exploit de día Cero**: Hace referencia a que no existen firmas de antivirus, ni parches sobre esta vulnerabilidad y puede ser explotada fácilmente por los atacantes.

Las definiciones relacionadas anteriormente son algunas de muchas de los términos que identifican este tipo de amenazas que debemos dar a conocer a los skateholders de la organización para que sepan cómo actuar ante esta situación y reportarlas de manera correcta y acorde, por esta razón es que se diseñan los planes de concienciación y sensibilización de las organizaciones.

EL diseño del plan de concienciación se estructura de la mano de la alta dirección el CISO encargado y los funcionarios, pero para esto sería importante que las organizaciones se planteen preguntas, con el fin de descubrir cuáles son esas problemáticas de seguridad y ciberseguridad y poder actuar como se menciona por IT Governance Institute en su libro de Information security governance en su capítulo 5, mencionando lo siguiente:

"los responsables de la gobernanza de la seguridad de la información pueden necesitar algunas preguntas iniciales que inviten a la reflexión y aumenten la conciencia para descubrir problemas de seguridad de la información y tener una idea inicial de lo que se está haciendo al respecto." [6]

El texto anterior de IT Governance es relevante para dar inicio con la construcción de los planes de concienciación en vista de las debilidades y falencias según los resultados obtenidos producto de una evaluación previa, generando la línea base de hacer la gobernanza bajo algunas de las preguntas que se relacionan a continuación:

- ¿La gerencia sabe quién es responsable de la seguridad? ¿El responsable lo sabe? ¿Todos los demás saben? [6]

Haciendo un pequeño análisis es una de las preguntas que genera valor y debería hacer los gerentes, presidentes y personal de la alta dirección esto puede notar muchas veces no conocer que son parte principal del proceso de seguridad, para que los demás responsables desde el nivel más bajo puedan estar involucrados generando una corresponsabilidad de colaborar en el proceso de seguridad de la información y apoyar de manera asertiva a los equipos interdisciplinarios de las organizaciones.

- ¿Las personas reconocerían un incidente de seguridad cuando lo vieran? ¿Lo ignorarían? ¿Sabrían qué hacer al respecto? [6]

Otra de las preguntas que es de gran valor a la hora de definir el plan de concienciación es saber si los funcionarios de la organización incluidos los de la parte de TI, tienen la capacidad de responder y argumentarla, debido a que en algunas ocasiones podemos tener sorpresas, en donde las áreas encargadas no saben cómo actuar o identificar este tipo de anomalías. Con esto se puede tener un análisis de brecha y actuar sobre este tipo de temas que son cruciales y de alto impacto al interior de las organizaciones.

- ¿Cuándo fue la última vez que la alta dirección se involucró en decisiones relacionadas con la seguridad? ¿Con qué frecuencia la alta dirección se involucra en el progreso de las soluciones de seguridad? [6]

La pregunta anterior también genera un gran valor ya que permite saber que tanto estamos teniendo presente la alta dirección en las decisiones de seguridad y ciberseguridad que impactan el negocio, en muchas ocasiones no basta con dar un reporte de cómo estamos y en que se ha avanzado, sino que los directivos de la alta dirección hagan parte del proceso y entiendan porque es tan importante su participación teniendo un entendimiento más detallado de los reportes entregados y comprender la razón de los resultados, a veces no se logra trasmitir la información por su nivel de tecnicidad a la hora de presentarlo.

Entre en las preguntas que se socializaron anteriormente tenemos muchas otras que nos entrega el IT Governance Intitute que podemos entrar a profundizar con los equipos de trabajo y ver la importancia de tener claro este punto de vista y de esta manera empezar a basarnos en el modelo de conciencia que se aplicara al interior.

Los objetivos del plan de conciencian deben ser claros y alineados con lo socializado anteriormente, se deben tener en cuenta los siguientes ejemplos:

- Dar a conocer cuáles son las amenazas a las que está expuesto el negocio.

- Concientizar la gestión e identificación de los riesgos de la organización.
- Conocer las políticas de seguridad y ciberseguridad definidas en la organización.
- Explicar la forma de reportar y a quien reportar una anomalía o amenaza de seguridad que comprometa los activos de información.
- Definir roles y responsabilidades de los colaboradores en el proceso.
- Identificar la estructuración del Gobierno seguridad y Ciberseguridad.

Estos ejemplos mencionados anteriormente son algunos que sirven para estructurar esos objetivos y socializarlos con los directivos para que de primera mano apoyen el proceso y puedan dar su aporte desde la línea de negocio y estratégica de la organización.

Las estrategias que se definan son las que permitirán que los colaboradores se interesen, estas pueden ser, conferencias, juegos, encuestas, webinars, entre otras que puedan incursionar acompañadas de las campañas de seguridad y ciberseguridad por medio de los wallpapers de escritorio, mails y demás medios de comunicación con los que cuenta la organización.

Uno de los impulsores en temas de concienciación como lo es el Instituto Nacional de Ciberseguridad de España conocido como (INCIBE) que promueve temas y herramientas para las organizaciones, donde da un kit para hacer todo el proceso y apoyarse de material de primera mano que en muchas organizaciones desconocen que pueden implementar de forma gratuita con el propósito de evitar y prevenir incidentes de seguridad y ciberseguridad que afectan a las organizaciones [14].

Finalizando el tema de concienciación es solo uno de los elementos que se puede incluir para fortalecer el gobierno de seguridad en la organización y es uno de los factores claves para que el eslabón más débil no sea el que rompa la cadena y poder crecer en el desarrollo de capacitaciones y fortalecimientos de los planes de conciencia al interior de las organizaciones y garantizar una mejora continua del gobierno de seguridad y ciberseguridad.

VI. MEDICIÓN - MEJORA CONTINUA

"Lo que no se mide, no se puede mejorar" esta frase, atribuida frecuentemente a Peter Drucker. Nos da una partida a lo que hace referencia el tema métricas y resultados, si no sabemos cómo estamos ni definimos niveles de cumplimiento ante un marco de referencia es difícil identificar nuestro nivel de madurez y si se están haciendo las cosas adecuadamente, es aquí donde hay que mejorar y nos sirve para saber si el gobierno de seguridad y ciberseguridad está dando cumplimiento a sus objetivos.

Según la ISO/IEC 27001 menciona que los indicadores son métricas generales que evalúan sobre la eficiencia o riesgo de un SGSI [10]. Cuando se habla de indicadores o métricas con un nivel más específico se debe dar alcance a tres conceptos importantes:

A. **KPI:** Es conocido como el indicador clave del desempeño. Una definición más técnica según la ISO es Indicadores Clave de Desempeño, conocidos comúnmente como KPI (Key Performance Indicator) cuando se quiere reflejar la adquisición de un resultado relevante para la actividad de la empresa *[10]*.

Según Sunil Bakshi en su artículo de ISACA menciona que los KPI y métricas son herramientas esenciales para la gerencia que son implementadas en todas las áreas del negocio. Hoy día, el uso de TI y tecnologías relacionadas por las empresas requiere de grandes inversiones de TI. Por lo tanto, los skateholders están interesados en confirmar que las inversiones de TI estén alineados estratégicamente, administrados efectivamente y ayudan en lograr las metas de negocio más comunes. Para asegurar que las expectativas de las partes interesadas se cumplan, la gerencia utiliza prácticas de Gobierno TI que están definidas por el estándar global por la Organización Internacional de normalización (ISO) ISO38500 y COBIT5 5 entre otros [15].

Para dar ejemplos de la definición de los KPI podemos verlo más adelante en la Ilustración 6.

B. **KRI:** Es conocido como el indicador clave de riesgo. Hablamos de Indicadores Clave de Riesgos o KRI (Key Risk Indicator), cuando una métrica muestre advertencias en relación con el riesgo situado en los ámbitos operacionales *[10]*.

Según el marco de COBIT5 menciona que para riesgo define los KRI como métricas capaces de mostrar que la empresa tiene o tiene una alta probabilidad de estar sujeta a un riesgo que excede el apetito de riesgo definido [16]. Es por esta razón que son fundamentales para la medición y el control de la optimización de riesgos y rendimiento. Estas métricas ayudan a informar eficazmente los resultados de rendimiento de la gestión de riesgos a los skateholders y permiten la administración con el fin de poder tomar decisiones informadas sobre la gestión de riesgos [17].

Dando alcance a ejemplos de KRI según el artículo de ISACA escrito por Rama, podemos observar que la Ilustración 5 nos da un alcance de alto nivel:

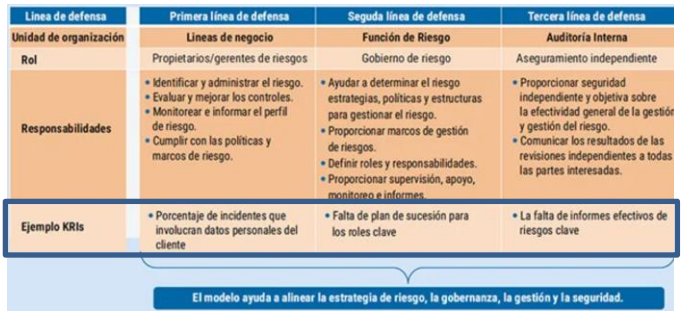

Ilustración 5 KRI para las líneas de defensa [17]

Estos son algunos de los KRI que pueden llegar a definir en el gobierno de seguridad enmarcando las líneas de defensa que se expusieron en el II capítulo del documento.

Según la ISO menciona algo que genera valor respecto a las diferencias y focos de los indicadores:

"Mientras los KPI se enfocan en datos históricos, los KRI o indicadores clave de riesgo se concentran en el pronóstico de lo que podría suceder, es decir, ayudan a anticipar problemas y oportunidades futuras, basándose en la observación de tendencias que puedan afectar a una organización." [10]

Para profundizar más en las diferencias de los KPI y KRI evidenciamos la definición de cada uno de ellos y su implicación e impacto en el negocio como se observa en la ilustración 6 la cual muestra muy detalladamente sus definiciones y alcances:

KRI	KPI	Implicación/impacto del negocio
Falta de plan de sucesión para los roles clave	Lanzamiento a tiempo del servicio o entrega del proyecto	La falta de respaldo para los roles clave identificados afecta la continuidad del servicio, lo que lleva a problemas de cumplimiento y posible incumplimiento de los acuerdos de nivel de servicio (SLA).
Porcentaje de incidentes que involucran datos personales del cliente	Cumplimiento de regulaciones, políticas o procesos	Esto indica un incumplimiento de las obligaciones de cumplimiento y puede llevar al escrutinio de los reguladores o los medios de comunicación, lo que puede afectar negativamente la reputación de la organización.
Número de servicios cancelados o retrasados debido a tiempos de inactividad de los servicios relacionados con la seguridad	Número de tiempos de inactividad del servicio relacionados con la seguridad	Los incidentes de seguridad que afectan a los sistemas críticos pueden causar la interrupción o degradación del servicio.
Porcentaje de aplicaciones/ sistemas empresariales que no son compatibles con un plan de respaldo	Número de aplicaciones/ sistemas empresariales que no son compatibles con un plan de respaldo	La falta de respaldo de datos para las aplicaciones/sistemas de negocios conduce a la pérdida de datos y afecta negativamente la continuidad del servicio en caso de interrupción.
Número de no conformidades detectadas en las pruebas/ auditorías de seguridad que quedan sin resolver más allá del período de tiempo planificado	Porcentaje de no conformidades detectadas en las pruebas de seguridad/ auditorías, pero no resueltas dentro del marco de tiempo planificado	El retraso en la solución de vulnerabilidades detectadas en las pruebas de seguridad/ auditorías hace que la organización sea un objetivo fácil para ataques maliciosos.
Número de incidentes de seguridad atribuidos a vulnerabilidades en sistemas de terceros/empleadoss	Gestión de terceros inadecuada	La información de la organización puede estar expuesta a riesgos por parte de terceros con una administración de seguridad de la información inadecuada.
Número de sistemas sin parches actualizados	Falta de un marco de tiempo adecuado para el tiempo de inactividad programado de los sistemas	El retraso en el parcheo de los sistemas hace que la organización sea un objetivo fácil para ataques maliciosos.
Falta de informes efectivos del riesgo clave	Falta de revisión de los procesos de gestión de riesgos	En ausencia de una revisión de los procesos de gestión de riesgos, estos procesos podrían continuar siendo ineficaces, lo que daría como resultado la no identificación de las vulnerabilidades/riesgos.

Ilustración 6 Implicación e Impacto de negocio de los KRI y KPI [17].

C. Balance Scorecare:

Son metas corporativas desarrolladas utilizando las dimensiones del cuadro de mando integral (CMI. En inglés: Balanced Scorecard, BSC) y representan una lista de objetivos comúnmente usados que una empresa puede definir por sí misma. Aunque esta lista no es exhaustiva, la mayoría metas corporativas específicas de la empresa pueden relacionarse fácilmente con uno o más de los objetivos genéricos de la empresa [16].

Como observamos en la ilustración 7 se identifican las perspectivas del Balance Scrorecard:

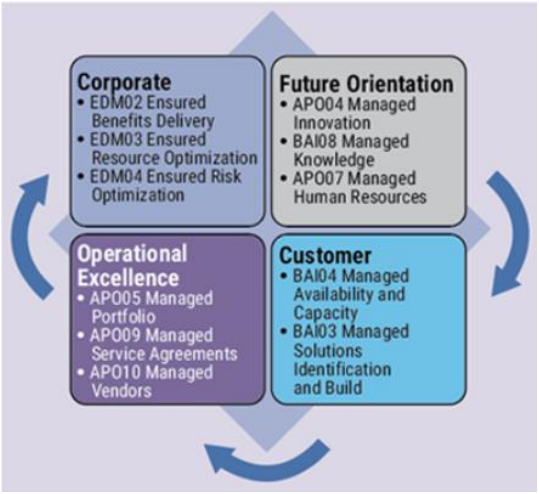

Ilustración 7 Perspectivas del BSC [18]

El balance Scorecard permite que las organizaciones tengan la visión general de la organización desde los cuatro frentes [18]:

- **Financiero:** Como es común toda organización mide su desempeño respecto a los indicadores económicos que ha definido la alta gerencia y directivos, permitiendo medir las utilidades y rendimientos sobre cada una de las inversiones que se realizan sobre el aseguramiento y protección de la información [18].

  Como es normal los directivos y alta gerencia quiere ver el retorno en la inversión de sus ingresos en temas de seguridad, en este caso particular puede ser variable ya que la seguridad no tiene un retorno sobre la inversión, por lo tanto, no van a obtener mayores ganancias o utilidades, lo que si van a tener es mayor aseguramiento en sus productos y servicios, mayor confianza de sus clientes y valor agregado en la aplicación de seguridad en su información. Esto podemos verlo en otro tipo de perspectivas.

- **Del Cliente:** Esta es una de las perspectivas que hace mover el negocio ya que esta ofrece mediciones sobre algunos aspectos relacionados a los clientes de la organización, permitiendo saber y medir los niveles de satisfacción, la retención de los clientes y la percepción de los nuevos [18].

  Con esto se hace un proceso de valoración en donde podemos identificar las fallas y aplicar al proceso de mejora continua para corregir y retar la organización a su crecimiento ante sus clientes y mejorar su imagen corporativa para los nuevos.

- **Procesos:** Hacen parte de la generación y el incremento del desempeño por medio de la identificación y medición [18]. Es donde se relacionan los procesos de seguridad y aseguramiento de cómo hacer este tipo de actividades dando cumplimiento a marcos y estándares técnicos como lo es la ISO 27001, COBIT5, ITIL entre otros.

  Dentro de esta perspectiva podemos definir métricas como nivel de cumplimiento en aseguramiento de los servicios ofrecidos, tiempo de respuesta en requerimientos de los clientes, nivel de acompañamiento y soporte al cliente.

- **De aprendizaje y crecimiento:** En esta perspectiva vamos a proyectar el crecimiento de la organización con base a sus infraestructuras [18]. Esta línea permite que se puedan generar planes de acción y mejora a las perspectivas anteriores ya que siempre se deben mejorar los procesos, aunque se cumplan con las metas ya que el negocio está en constante evolución y cada día deben crearse más estrategias de negocio alineados al aseguramiento de la información.

Además, cuenta con una meta por cada uno de los cuatro frentes que se definen, con el fin de poder cumplir objetivos alineados al negocio [18].

Los indicadores de desempeño son una parte clave para cada una de las perspectivas descritas ya que permiten que la organización pueda saber si su estrategia está acorde con lo esperado o si definitivamente debe replantearse.

El Balance Scorecard siempre estará presente para el gobierno de Seguridad ya que muchas de sus estrategias van alineadas al negocio para poder consolidarlo con más fuerza en la organización.

VII. CONCLUSIONES

El gobierno de seguridad y Ciberseguridad debe estar inmerso en todos los procesos de la organización para poder tener una gobernanza acorde a lo que buscan las organizaciones asegurando su activo más valioso como lo es la información.

Como se logró identificar en los capítulos II, III, IV, V y VI se menciona el apoyo y la participación de la alta gerencia y directivos, para que el gobierno de seguridad pueda cumplir con sus requisitos y establecerse de una forma más estructurada y que su gobernanza sea respaldada para dar cumplimiento a los lineamientos internos y externos que deben ser considerados por la organización, aplicando los marcos de referencia y buenas prácticas.

Como se describió y especifico en el capítulo V del documento la concienciación y respaldo de los directivos es fundamental para que se pueda optar por un buen gobierno donde todos los funcionarios se convierten en un apoyo para fortalecer los procesos identificar brechas y riesgos que comprometan servicios, clientes y la información que debe garantizar su correcto aseguramiento.

Finalmente, cada uno de los capítulos es una parte importante que debe cumplirse y establecer en la organización para que el gobierno de seguridad tome una gobernanza al interior y pueda definir lineamientos que permitan dar alcance a las necesidades del negocio con el aseguramiento de las infraestructuras, personal y activos de información.

VIII. REFERENCIAS

[1] ISACA, «Isaca.org,» [En línea]. Available: https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance. [Último acceso: 10 12 2022].

[2] NIST, «NIST CYBERSECURITY FRAMEWORK,» [En línea]. Available: https://www.nist.gov/cyberframework/framework. [Último acceso: 24 10 2022].

[3] NIST, «Primeros pasos de NIST Marco de ciberseguridad: Guía de inicio rápido,» [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf. [Último acceso: 24 10 2022].

[4] E. Pernet, «Un modelo sistémico para el diagnóstico del estado de madurez del Gobierno, Riesgo y Cumplimiento en las organizaciones,» Newport University, United States of America, 2013.

[5] MinTIC, «articles-5482_Modelo_de_Seguridad_Privacidad,» [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-

5482_Modelo_de_Seguridad_Privacidad.pdf. [Último acceso: 26 10 2022].
[6] IT Governance Institute, «Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd Edition,» de Information Security Governance, Rolling Meadows,, Leading The IT Governance Community, 2006, pp. 48-52.
[7] J. R. Yupanqui y S. Bayona Oré, «Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su cumplimiento.,» RISTI (Revista Ibérica de Sistemas y Tecnologías de Información), Lima, 2017.
[8] RAE, «RAE,» [En línea]. Available: https://dle.rae.es/lineamiento. [Último accesso: 2022 11 01].
[9] IT Governance Institute, Cobit security baseline : an information security survival kit, Rolling Meadows: IT Governance Institute, 2004.
[10] INCONTEC, TECNOLOGIAS DE LA INFORMACIÓN TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS, Bogotá: ICONTEC, 2013.
[11] J. Dr. Mendivil Caldentey, U. Dr Borja Sanzs y A. Dra Miren Gutiérrez, «REcyt,» [En línea]. Available: https://recyt.fecyt.es/index.php/pixel/article/view/91640/67683. [Último acceso: 2022 11 02].
[12] J. Mendivil, U. Borja Sanz y A. Miren Gutiérrez, «PÍXEL-BIT,» 07 01 2022. [En línea]. Available: https://recyt.fecyt.es/index.php/pixel/article/view/91640. [Último accesso: 12 11 2022].
[13] ISACA, «Advance Persistent Threats How to Manage the Risk to Your Business,» Isaca, 2013, pp. 24-46.
[14] INCIBE, «INCIBE,» [En línea]. Available: https://www.incibe.es/protege-tu-empresa/kit-concienciacion. [Último acceso: 2022 11 02].
[15] S. Bakshi, «ISACA,» 12 06 2017. [En línea]. Available: https://www.isaca.org/es-es/resources/isaca-journal/issues/2016/volume-6/performance-measurement-metrics-for-it-governance. [Último acceso: 2022 11 04].
[16] ISACA, COBIT 5 FOR RISK, USA: ISACA, 2013.
[17] R. L. S. Tammineedi y ISACA, «ISACA,» 22 06 2019. [En línea]. Available: https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-4/integrating-kris-and-kpis-for-effective-technology-risk-management. [Último acceso: 2022 11 04].
[18] I. Ioannis Routsis, «ISACA,» [En línea]. Available: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/lost-in-the-woods-cobit-2019-and-the-it-balanced-scorecard. [Último accesso: 11 11 2022].
[19] ISACA CSX, «Cybersecurity Fundamentals Study Guide, 2nd edition,» de Cybersecurity Fundamentals Study Guide, 2nd edition, ISACA, 2017.

Holber S. Hernández G. Ingeniero en Sistemas, próximo a obtener el título de Especialista en Seguridad Informática, cursando Maestría en Seguridad Informática y Comunicaciones, certificado como Auditor Interno en ISO 27001:2013, con una trayectoria de más de 5 años en diferentes sectores públicos y privados (Banco, Tecnología, Servicios y Outsourcing), con experiencia en Gobierno de Seguridad y Ciberseguridad, aseguramiento, arquitectura y diseño de controles de seguridad y ciberseguridad, aplicaciones, administración de software y herramientas de seguridad, definición de posturas de ciberseguridad y manejo de indicadores.