CULPABILIDAD O RESPONSABILIDAD DE LA JUNTA DIRECTIVA EN EL RIESGO CIBERNÉTICO.

Por: Ing. Henry Wilson González B. Octubre-2019

[B][1] ¡En la anterior sesión hablamos de algunos elementos básicos del Riesgo Cibernético que se encuentran en el vado de este módulo de riesgo. Como complemento correlacionado hoy pretendo discernir con ustedes la pregunta que quedo en el tintero sin contestar ¿De quién es la responsabilidad del Riesgo Cibernético? Para construir una respuesta a esta pregunta, voy a activar sus conocimientos previos mediante la siguiente afirmación, un tanto grotesca de mi parte, pero muy clara desde mi experiencia real y profesional, no académica. Advierto que, quien no esté de acuerdo con ella, la puede refutar pero solo con argumentos, no acepto apelaciones emocionales o hábitos de países tercermundistas normalmente aceptados!

¡No hay nada mejor en el mundo que pertenecer al "Club de Colosales Egos" también llamada Junta Corporativa[2], que se diferencia del gran club, por las siguientes características: i) Anudan muy pocos de ellos en un solo órgano que los resguarda, ii) Todos son selectos, es decir, que se reputan como los mejores de su especie, iii) Conocen y hablan con propiedad de todos los temas, iv) Tienen responsabilidades individuales y grupales dentro de su órgano pero es el único club donde la inobservancia o incumplimiento de dichas responsabilidades no conlleva culpabilidades, generalmente estas últimas serán siempre señaladas a sus inferiores, v) Se reúnen rigorosamente en periodos pre establecidos, vi) Es el único club donde sus miembros no pagan cuota de afiliación o mantenimiento en el club, sino que por el contrario les pagan por asistir al mismo, vi) Gozan de la mayor credibilidad y respeto de todos sus inferiores, y finalmente.. vii) Un miembro de este club, entre más "Juntas Corporativas" pertenece más proclive y venerado será para las empresas!

¡Veo que todos quedaron absortos con mi definición de las características de las Juntas Corporativas, en el camino validaremos si tengo la razón al respecto o estoy siendo muy enérgica con la misma, por ahora empecemos por describir el contexto de lo ocasiona el no cumplimiento de las responsabilidades, "Las Pérdidas"!

Es un hecho que los riesgos independientemente de su forma, contienen pérdidas en el momento que se materializan. Estas pérdidas pueden tener varios orígenes a saber: Por eventos de riesgo operativo, sanciones pecuniarias por incumplimiento a la normativa vigente sobre los riesgos del lavado de activos y financiación del terrorismo, multas por desacato, mal uso premeditado o no de la información de datos personales de las contrapartes, es decir, de clientes, empleados, proveedores o socios, sanciones por impericia o ausencia de la eficiencia del sistema de control interno, entre otros. Sin embargo, aquí hablaremos únicamente de las pérdidas derivadas del Riesgo Cibernético.

Si las pérdidas asociadas al riesgo cibernético son:

1.- Perdida de propiedad intelectual
2.- Perdida de sus planes comerciales
3.- Destrucción o alteración de datos

---

[1] Nota del autor: Este documento es tan solo un ensayo que recrea las conversaciones entre "Baucis" la Directora del MBA de Alta Gerencia – Módulo de Riesgo Empresarial, en una prestigiosa Universidad Colombiana. "Baucis" será identificada en todo el texto como [B]. De otra parte aparece "Filemón" el participante - estudiante del MBA, quien es un ejecutivo del equipo directivo en una organización mediana y que durante todo el texto se identificará como [F]. En algunos casos se utilizara lo siguiente [O] para identificar "Otros" estudiantes del MBA, que también hacen preguntas o reflexionan sobre el tema en cuestión. Las conversaciones se desarrollan al interior del aula de clase, mientras "Baucis" evoluciona en su cátedra. El origen de los nombres obedece a la mitología griega donde describen quienes fueron Baucis y Filemón.

[2] La Junta Corporativa está conformada por: El Gerente y/o Representante Legal y Miembros de la Junta Directiva o de quien haga sus veces. (Puede en algunos casos incluir al Revisor Fiscal y Al Oficial de Cumplimiento)

4.- Interrupción de la infraestructura crítica
5.- Exponerse a sanciones reglamentarias
6.- Disminución de la confianza pública e interna de las partes interesadas

Fácilmente se puede colegir que las dos últimas pérdidas son producto causal correlacionado con pérdidas precedentes. Las cuatro primeras pérdidas obedecen a eventos que se originan por el incumplimiento de responsabilidades asociadas a temas de tecnología, es decir, que tienen un origen de carácter cibernético, dado que existen personas externas a la entidad como hackers o personal altamente calificado en tecnologías invasivas con objetivos de ganancia financiera rápida y secuestro de información con fines delictivos.

> "Muchas corporaciones podrían tildar estos eventos como simplemente un costo frustrante de hacer negocios. Hoy en día, las corporaciones están asediadas por atacantes que forman parte de equipos ultra sofisticados que implementan malware cada vez más dirigido contra sistemas y personas, atacando de manera furtiva en múltiples etapas. Estos ataques, a veces denominados amenazas persistentes avanzadas (APT, por sus siglas en inglés)
>
> Una de las características determinantes de estos ataques es que pueden penetrar en prácticamente todos los sistemas de defensa perimetral de una empresa, como los cortafuegos o los sistemas de detección de intrusos. Se calculan meticulosamente estos ataques para asaltar a un objetivo específico, y los intrusos buscan múltiples vías para explotar las vulnerabilidades en todas las capas de seguridad hasta lograr sus objetivos. La realidad es que si un atacante sofisticado tiene en la mira los sistemas de una compañía, casi con seguridad los violará. Esto no significa que la seguridad sea un imposible, solo significa que la ciberseguridad debe ser más que simplemente la seguridad perimetral basada en TI. Dado que los ataques se han vuelto más sofisticados, las defensas deben volverse más sofisticadas"[3]

Las pérdidas por Riesgo Cibernético a simple inspección y casi de forma automática son catalogadas como una problemática y responsabilidad a solucionar por parte del área de TI., sin embargo, en la clase anterior (Ver ensayo clase No. 5) se exploró esta afirmación y se afinó lo siguiente como hechos contundentes.

1.- Las acciones de ciberseguridad óptimas, que garanticen controlar o mitigar el Riesgo Cibernético no están dentro del componente presupuestal del área de TI
2.- Las inversiones en arquitectura tecnológica son costosas y tienden a ser frecuentes y que no acaban, porque la velocidad del cambio en lo tecnológico es muy acelerado.

[3] Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas – OEA – Pág. 10 - versión estadounidense del Manual de 2017

3.- El Riesgo Cibernético no es una responsabilidad exclusiva del área de TI, sino que por el contrario, es una responsabilidad multidisciplinar o multifuncional, es decir, deben participar muchas otras áreas más.

Esto no es un silogismo, pero al tratar de aplicarlo demuestra que si tiene esa deducción lógica, es decir, las premisas deducen indefectiblemente que la Junta Corporativa es quien debe asumir estas responsabilidades.

Permítanme adicionar otros elementos de juicio mediante las siguientes preguntas, para entender la deducción explícita que nos lleva a la respuesta de la pregunta principal. ¿De quién es entonces la responsabilidad del Riesgo Cibernético?

Preguntas orientadoras:

¿Qué organismo gestiona, justifica, aprueba y monitorea los rubros de los proyectos de inversión en la organización?
¿Quién determina y aprueba los presupuestos funcionales?
¿Quién debe velar por cumplir con la normativa vigente y los requerimientos de Ley, a fin de evitar que la empresa este expuesta a sanciones reglamentarias?
¿Qué organismo debe procurar no tener una disminución de la confianza pública e interna de las partes interesadas?

La respuesta a estas preguntas es unívoca y no admite ambigüedad, es la Junta Corporativa la responsable del Riesgo Cibernético. De otra parte y como resultado de lo anterior el área de TI, contiene una responsabilidad indirecta y hasta exigua frente a dicho riesgo, no significando esto; que no es el actor principal del diseño, implementación y monitoreo de controles, (ciberseguridad) en la medida de sus capacidades y circunstancias de cara al Riesgo Cibernético.

Hagamos aquí una digresión al tema Responsabilidad – Riesgo Cibernético para entender su correlación; clara, concreta y precisa con el concepto “Culpabilidad”

La pregunta ahora es: ¿No cumplir con la responsabilidad es afrontar la culpabilidad de lo que pasó o pueda pasar?

Discutamos el contexto jurídico de la palabra “Culpabilidad” para lograr entender las responsabilidades de la Junta Corporativa y su relación con la culpabilidad al no ejercer, efectuar, controlar, decidir o hacerse responsable de las funciones asignadas por los organismos de vigilancia y control del estado, de cara al tratamiento y control de los disímiles riesgos al que está expuesto la empresa en especial lo relativo al Riesgo Cibernético.

Las personas que conforman este conglomerado social, llamado Junta Corporativa tienen la obligación de dispensar todo el cuidado y atención para no generar daño no intencional a la organización por el no cumplimiento de sus funciones. Pero cuando se incumple este precepto y se da a lugar a un resultado dañoso por un

actuar imprudente o negligente podrá deducirse una responsabilidad penal para quien así actuó no a título de dolo pero si a título de culpa.

En una sociedad de riesgos aceptados, la culpa consiste en llevar el riesgo de la acción, más allá de los límites socialmente admitidos.[4]

La definición jurídica del concepto "Culpa" en Colombia está determinada así:

> "La conducta es culposa cuando el resultado típico es producto de la infracción al deber objetivo del cuidado y el agente debió haberlo previsto por ser previsible o habiéndolo previsto confió en poder evitarlo."[5]

1.- Entiéndase la Junta Corporativa al: Gerente, Representante legal, Directores, Miembros de la Junta Directiva o quien haga sus veces.
2.- Las Responsabilidades asignadas por los entes de control, hace referencia a las responsabilidades establecidas en la reglamentación para los sistemas de riesgo como: Saro, Sagrlaft, Sci, Sarc, Sarl, PDP-Ley 1581, entre otros, por las correspondientes superintendencia de control y vigilancia.

Responsabilidad Vs Culpabilidad · SCI · Sistema de Control Interno – HW Risk – Derechos Reservados de Autor – Versión 1 –Sep_2019

Existen dos tipos de culpa que se manejan para estos casos donde se correlaciona las acciones dejadas de hacer y que conllevaron a un acto dañoso, la culpa consiente o con representación y la culpa inconsciente o sin representación. Para entenderlo mejor ilustrémoslo en el tema que nos compete.

[4] Sentencia 26027 del 30 Mayo-2007 - Sala de Casación Penal de la Corte Suprema de Justicia en Colombia referente al concepto de "Culpa" - Magistrado Yecid Ramírez Bastidas.
[5] Ley 599 del 2000 Derecho penal colombiano.

La culpa sin representación significa que la conducta de las personas que conforman el estamento de la Junta Corporativa deben haber previsto los riesgos a que estaban expuestos porque son previsibles, es decir, dichos miembros podrán ser sancionados por no haber previsto lo que sabían que podía pasar.

La culpa con representación implica para los miembros de una Junta Corporativa que habiéndoles explicado y expuesto las pérdidas derivadas de cada riesgo para la entidad, su comportamiento es representado como un resultado antijurídico dado que hubo materialización de pérdidas.

En este caso ellos actuaron de forma inadecuada y confiaron indebidamente en poder evitar los eventos mediante una estrategia de seguir actuando de la misma forma y asumir los riesgos con recursos de la sociedad en el mismo momento en que se presentan. Es claro que bajo su conocimiento ellos podrían haber evitado los riesgos, pero su actuar los indujo a tomar la decisión de esperar que la probabilidad de ocurrencia de dichos riesgos no los cobijara. Juega aquí un papel importante el concepto de apetito desmedido al riesgo.

De otra parte hay tres preceptos que deben ser tenidos en cuenta para determinar si la Junta Corporativa al no cumplir con sus responsabilidades respecto al tratamiento de los riesgos podría ser declarados culpables por las pérdidas incurridas.

El primero hace referencia a la inobservancia del deber objetivo de cuidado, es decir, actuar de manera imprudente o negligente o con impericia, respecto a las decisiones que debía tomar para el tratamiento de los riesgos. El segundo se desprende del primero, que significa que se causan resultados dañosos para la entidad en este caso perdidas económicas y el tercero comprende el análisis de causalidad entre los dos primeros; establecer la relación causa efecto que derivo en la pérdida incurrida, en algunos casos esta relación de causalidad podría ser tautológica, es decir, la causa genero el efecto y viceversa, pero siempre es lo mismo.

En Colombia existen cuatro factores generadores de culpa a saber:

1.- La imprudencia: Entendida como la ausencia de cautela o moderación o discernimiento, al afrontar un riesgo de manera innecesaria pudiendo evitarse. (Aplica aquí nuevamente el concepto de apetito desmedido al riesgo)

2.- La negligencia: Implica una falta de actividad que produce daño, es decir, el no hacer para evitar resultados dañosos, es sinónimo de descuido. (Sucede muy frecuentemente cuando no se atienden las responsabilidades derivadas de sus cargos por los miembros de la Junta Corporativa)

3.- La impericia: Asumida como la carencia de capacidad, de idoneidad y de experiencia, consideradas como habilidades mínimas requeridas para el desarrollo de actividades que pueden representar riesgo, especialmente en aquellos

conocimientos técnicos que se requieren para tomar las mejores decisiones. (Los Riesgos Cibernéticos se ven muy afectados por este factor y por ello los miembros de la Junta Corporativa se desentienden de esta responsabilidad y la delimitan como una responsabilidad exclusiva del área de tecnología)

4.- La inobservancia: Entendida como el no atender a los reglamentos u órdenes, es el caso de la reglamentación en los sistemas de riesgo que establece principios y límites esperados a la conducta de los miembros de la Junta Corporativa para el desarrollo de sus actividades.

[B] ¡A la altura de esta exposición ya se ven muchas manos arriba con ganas de discutir y debatir mi tesis principal, lo cual en todo caso enriquece la construcción del conocimiento objeto de esta cátedra en este tema tan particular. Bueno veamos, pues, algunas intervenciones – Preguntas contextualizadas para entenderlas mejor - Ok.

[O] ¡Las pérdidas asociadas al riesgo Cibernético como: pérdida de la propiedad intelectual, perdida de sus planes comerciales, destrucción o alteración de datos, interrupción de la infraestructura crítica, son, sin temor a equivocarme son problemas del área de TI, dejar que se roben archivos o documentos de la propiedad intelectual de la compañía, que roben los planes comerciales, que suceda destrucción o alteración de los datos o que interrumpan la arquitectura tecnológica, es su responsabilidad que no suceda, entonces no es cierto que exista una responsabilidad exigua o escasa del área de TI como usted lo llama!

[B] ¡Como dirían los abogados en el ejercicio de su disciplina “Ha Lugar” el comentario. – Salvo que lo que está sucediendo o sucedió, tiene origen en una solicitud de mejora a la arquitectura tecnológica de la empresa que no fue atendida o aprobada.

[F] ¡Unido al planteamiento de mí compañero, no puede ser una responsabilidad de la Junta Corporativa, si la siguiente situación tiene la empresa: pocas capas de seguridad perimetral, cortafuegos obsoletos o inservibles, bajo nivel de sistemas de detección de intrusos en la red, malware que lograron implementar los hackers, entre otros. Esto es un conocimiento técnico de los ingenieros de la tecnología de la información, que nosotros los miembros de la Junta Corporativa desconocemos en su gran mayoría!

[B] ¡Ha Lugar! Salvo que se cuente con una mala preparación técnica de los funcionarios del área de TI, que tiene dos fuentes de origen excluyentes entre sí: Primera un Gerente o Jefe de TI que nunca se preocupó por las capacidades y destrezas del personal a su cargo. Segunda una solicitud de formación y capacitación de los funcionarios de TI no atendida por la Junta Corporativa. El primer caso es fácil de solucionar. ¡Despedir al Gerente o Jefe de TI!, el segundo……

[O] ¡Para ilustración de todos y de usted Baucis, “El Derecho Penal” es la rama del derecho que establece y regula el castigo de los crímenes o delitos, a través de la imposición de ciertas penas, entre ellas la prisión. El derecho penal asocia a la realización de determinadas conductas, llamadas delitos, penas y medidas de seguridad como consecuencias jurídicas! Por lo anterior me llama la atención que usted hable de culpabilidad desde la óptica del derecho penal, como si nosotros los miembros de la Junta Corporativa o como usted lo denomino de forma peyorativa el “Club de Colosales Egos” obráramos de mala fe o con conductas delictivas y fuera de la Ley!

[B] ¡Distinguido abogado! ¿Logre llamar su atención con el tema?

[O] ¡No de la mejor forma, pero sí, lo logro!

[B] ¡Ok – esa era la intención. Sin embargo, favor respóndame si estoy o no, en lo cierto con la siguiente afirmación. “Si en Derecho el “Patrimonio” es un bien jurídico, susceptible de pérdida y las malas conductas originadas por negligencia, inobservancia, impericia o imprudencia, ocasionan pérdidas económicas a los inversionistas de una empresa, estas conductas son punibles por la culpa asociada a ellas”

[O] ¡Su afirmación es clara y precisa, ahora entiendo para donde va usted con su disertación y estaría de acuerdo!

[F] ¡Ahora si es claro el concepto de responsabilidad y por ende la culpabilidad de los miembros de las Juntas Corporativas en relación a los riesgos, en especial al Riesgo Cibernético! Pero ahora me asalta una nueva pregunta ¿La culpa ante quién?, si la Junta Corporativa es quien define sus reglamentos y conductas esperadas, entonces, ¡No hay culpables!

[B] ¡Bueno en empresas pequeñas y medianas esto puede ser cierto, aunque no siempre, pero no hay que olvidar la Asamblea General de Accionistas o reunión de socios, como se quiera denominar. Es con ellos que sí existe una responsabilidad directa, pues ellos, son los que invierten su capital y esperan una retribución económica aceptable por la organización y no una relación de pérdidas incurridas con justificación o sin ella!

[O] ¿Si entendí de forma correcta su exposición entonces debería concluir que quienes conformamos los equipos directivos de las organizaciones debemos volvernos expertos en temas de tecnología a fin de poder preguntar si las tareas asociadas al área de TI se están haciendo de forma correcta y oportuna para no correr el riesgo de materialización de pérdidas debido al Riesgo Cibernético?

[B] ¡No, no es responsabilidad de los miembros de la Junta Corporativa convertirse en expertos en TI, pero si deben saber qué preguntar al departamento de TI, para mejorar su comprensión del Riesgo Cibernético y poder establecer ¿Cuál es el grado de exposición e impacto financiero al que está expuesto la empresa? Además, las juntas deben ejercer el liderazgo y el compromiso necesarios, supervisando de forma proactiva y responsabilizando a la Gerencia y a los directores o jefes de área como responsable, de lograr que la protección de la organización contra el ciberataque sea una prioridad![6] Finalmente a continuación pongo sobre la mesa los 5 principios definidos en el manual precitado con anterioridad, que son las mejores recomendaciones para las Juntas Corporativas respecto al Riesgo Cibernético.

Si el riesgo cibernético contiene las perdidas enunciadas, entonces ¿Qué debe hacer una Junta Corporativa para inhibir esta situación? es ahora la pregunta a resolver.

La OEA – Organización de los Estados Americanos en conjunto con la Internet Security Alliance, desde el año 2017 consientes de las implicaciones del riesgo cibernético han preparado un documento denominado "MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS" el cual me permito ilustrar y comentar y en algunos casos inferir sobre la realidad que él, muestra que en algunos de sus componentes, no sé, si realmente aplica al contexto colombiano o sencillamente es un simple saludo a la bandera y su implementación en Colombia no es viable o procedente, sin embargo, es un documento muy valioso e ideal para llamar la atención de las Juntas Corporativas y su responsabilidad frente al riesgo cibernético.

Define el documento unos principios fundamentales a cumplir por las Juntas Corporativas que es necesario entender y escrutar sus implicaciones uno a uno.

Principio 1[7]
Los directores deben comprender y abordar la ciberseguridad como un problema de gestión de riesgos en toda la empresa, no solo como un problema de TI.

Lo anterior es verdadero si y solo sí:

¡Es un hecho que..!
1.- La ciberseguridad de la información es un problema meramente técnico.
2.- Los problemas de tecnología, relacionados con la ciberseguridad es una responsabilidad de TI.
3.- Los departamentos o áreas de TI, trabajan sin autoridad presupuestaria y con recursos limitados.

[6] Documento de la OEA – Critical Infrastructure Protectión in Latin América and the Caribbean - 2018
[7] Documento de la OEA – Organización de los Estados Americanos en conjunto con "Internet Security Alliance" - 2017 - Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas – Páginas 12 a 24. - Se recomienda leer con atención en este documento, para mayor ampliación sobre el contexto, cobertura y alcance de cada principio referido en este ensayo del autor.

4.- Las unidades orgánicas funcionales o unidades de negocio diferentes al área de TI, se sienten desconectadas de tener responsabilidad de la seguridad de sus propios datos.
5.- La responsabilidad de la seguridad e integridad de los "Datos" de las unidades de negocio recae como una responsabilidad delegada a TI, entonces, esto inhibe el análisis crítico de la información y por ende dificulta la implementación de estrategias de seguridad efectiva.
6.- Las empresas que invierten mucho en innovación de TI, tratan que las nuevas infraestructuras tecnológicas sean cada vez más importantes para el soporte de la estrategia y la operación comercial.

El análisis de causalidad permite inferir de lo anterior que los riesgos cibernéticos deben evaluarse de la misma manera en que una organización evalúa la seguridad física de sus activos humanos y físicos y los riesgos asociados con su posible compromiso. En otras palabras, la ciberseguridad es un problema de gestión de riesgos en toda la empresa que debe abordarse desde una perspectiva estratégica, económica, interdepartamental e interdivisional[8]

Principio 2
Los directores deben entender las implicaciones legales de los riesgos cibernéticos según se relacionan con las circunstancias específicas de su empresa.

Este principio refuerza el alcance y la cobertura de este documento específicamente en lo que atañe a la responsabilidad versus la culpabilidad, dado que describe con precisión y claridad los efectos sobre la Junta Corporativa cuando se toma a la ligera la atención del Riesgo Cibernético.

> "Las juntas deben estar al tanto de las cuestiones de responsabilidad actuales que enfrentan sus organizaciones y, potencialmente, los directores y dueños de empresas familiares y accionistas mayoritarios uno a uno. Por ejemplo, los ataques de alto perfil pueden generar demandas, incluidas demandas colectivas de accionistas y clientes, y podrían llevar a acciones de cumplimiento normativo. Los reclamantes también podrían alegar que la junta directiva de la organización descuidó su deber fiduciario al no tomar las medidas suficientes para confirmar la idoneidad de las protecciones de la empresa contra las violaciones de datos y sus consecuencias.."[9]

Este principio no debe asumirse como ideal, por el contrario sugiere el texto precitado realizar tareas muy puntuales y concretas a fin de "Demostrar" la gestión y proactividad de la Junta Corporativa y con ello mitigar la posibilidad de ser "Señalados" como responsables del descuido que desencadeno en las pérdidas.

Estas tareas se resumen de la siguiente forma:

[8] Ibídem.
[9] Ibídem.

Mantener un registro sistemático en actas que así lo demuestren, de los temas tratados en cada reunión donde salió a relucir hechos o ideas relacionadas con el Riesgo Cibernético, resaltando en las mismas las decisiones que el órgano tomo como acciones de ciberseguridad

Delegar en aquel miembro de la Junta Corporativa que demuestra mayor destreza en temas relacionados con la tecnología que este al pendiente e informado sobre las tendencias de la tecnología y los requisitos asociados a las acciones de ciberseguridad en la industria o sector económico al que pertenece la empresa. Lo anterior con la finalidad de discutir las afectaciones que esto podría ocasionar a la entidad y definir con la oportunidad requerida las acciones de propias en ese sentido.

Debe ser una tarea concurrente y sistémica el análisis de la evolución del Riesgo Cibernético, estado actual, eventos ocurridos, impactos posibles, planes de acción, medidas contingentes establecidas y hasta una sana paranoia de lo que podría pasar, como están preparados, qué se puede hacer como contingencia dos y en especial un informe detallado del resultado de las pruebas del PCN – Plan de Continuidad del Negocio.

En este último punto juega un papel muy importante para la Junta Corporativa dado que, al resolver la siguiente pregunta. ¿Qué manifestó el(los) organismos de control interno y externo, llámese Revisoría Fiscal o Auditoria de Control Interno o quien haga sus veces, frente a la prueba del PCN. Estos organismos deben participar de forma activa en estas pruebas del PCN y rendir un informe dirigido a la Junta Corporativa. Este informe demuestra con certera evidencia lo que está pasando con las medidas de ciberseguridad implementadas y su relación con los planes de contingencia a todo nivel, como también la efectividad de las acciones emprendidas por la Junta Corporativa en este sentido.

Parte del trabajo a realizar en el punto anterior, incluye la definición por parte dela Junta Corporativa sobre lo que se puede o no decir, en aquellos casos donde se ha materializado un ataque cibernético, debe existir un protocolo bien definido de quien puede socializar los eventos, cuál debe ser la forma de hacerlo, quien será el público receptor de esta información y hasta donde se deben entregar los detalles de lo que paso y la divulgación de la situación.

Principio 3

Las juntas deben tener un acceso adecuado a la experiencia en ciberseguridad y se le debe proporcionar un tiempo regular y adecuado a las discusiones sobre la gestión de riesgos cibernéticos en las agendas de las reuniones de la junta.

> La mayoría de las Juntas Corporativas en América Latina tienen una comprensión "inicial" o "formativa" de la ciberseguridad, lo que significa que tienen una comprensión mínima o nula de la ciberseguridad y los deberes fiduciarios relacionados, o tienen cierta conciencia de los problemas cibernéticos, pero no de cómo los riesgos podrían afectar a sus organizaciones.[10]

Este es uno de los aspectos más complejos de solucionar en la conformación de las Junta Corporativa dado que no siempre se cuenta con el especialista o experto en temas de tecnología que pueda orientar, verificar y dar soporte al organismos, frente a los informes presentados por la Gerencia de Tecnología o quien haga sus veces, debido a la complejidad del tema. Como lo discutimos con anterioridad aquí lo importante es saber que preguntar para poder saber que tan expuesta está la empresa de cara a la materialización del Riesgo Cibernético.

Se plantean algunas acciones de mejora para que las juntas aborden esta problemática y puedan intervenir con mucha fuerza en las decisiones asociadas a las acciones de ciberseguridad y sus componentes, entre estas acciones encontramos las siguientes: Mejorar el acceso a la experticia en ciberseguridad, lograr acceso a una experticia adecuada en ciberseguridad y mejora de los informes de gestión que vienen del área de tecnología con destino a la junta, este último debe incluir las acciones concretas que están haciendo las áreas funcionales directas del negocio, diferentes al área de TI, frente a su responsabilidad con los datos y la información de las partes interesadas.

[10] Ibídem

Principio 4

Los directores de la junta deben establecer la expectativa de que la gerencia establecerá un marco de gestión de riesgo cibernético para toda la empresa con personal y presupuesto adecuados.

> La tecnología integra a las organizaciones modernas, ya sea que los trabajadores estén al otro lado del corredor o al otro lado del mundo. Pero, como se señaló anteriormente, las estructuras de presentación de informes y los procesos de toma de decisiones en muchas empresas son legados de un pasado, donde cada departamento y unidad de negocios toman decisiones de manera relativamente independiente y sin tener en cuenta que la interdependencia digital es un hecho de los negocios modernos. Los directores deben buscar garantías de que la gerencia está adoptando un enfoque apropiado de ciberseguridad en toda la empresa.[11]

La gestión del riesgo debido a todo lo que hemos hablado, sumado a otros riesgos como el operativo, lavado de activos, protección de datos personales, entre otros que existen. NO debe verse al interior de la organización, con una paranoia desmedida, porque cuando esto sucede, se llega rápidamente a la "Histeria" frente al riesgo. En otras palabras y para decirlo en romance llano es un gran error ver a la gestión del riesgo como costos adicionales, actividades complejas y pesadas, inoportunas y hasta fastidiosas porque terminan encasillando a la gestión del riesgo como un nuevo "centro de costo" lo cual perjudica el accionar de la gestión del riesgo de forma integral.

Principio 5

La discusión de la junta directiva sobre el riesgo cibernético debe incluir la identificación de qué riesgos evitar, cuáles aceptar y cuáles mitigar o transferir a través de un seguro, así como planes específicos asociados con cada abordaje.

> "Al igual que con otras áreas de riesgo, la tolerancia al riesgo cibernético de una organización debe ser coherente con su estrategia y objetivos comerciales. Cuando una organización analiza su riesgo cibernético, debe hacerlo como parte de su evaluación general de riesgos, ubicando adecuadamente a los cibernéticos en el contexto de otros riesgos. La asignación de recursos de seguridad es una función de equilibrio entre los objetivos de negocio y los riesgos inherentes.."[12]

Finalmente este principio cierra el círculo de toda la exposición, cohesiona de forma adecuada con el planteamiento que se ha pretendido presentar sobre la responsabilidad de la Junta Corporativa y su relación con el Riesgo Cibernético.

Si se cumplen estas premisas la Junta Corporativa tendrá una mejor posición dentro del proceso de toma de decisiones respecto a qué nivel de tolerancia o apetito al

[11] Ibídem
[12] Ibídem

riesgo quiere manejar, que riesgos debe transferir y porque razón hacerlo, y donde debe emprender acciones de forma inmediata para ejercer un verdadero control a la gestión del riesgo como una visión global y no local.

[B]

¡El Riesgo Cibernético contiene una claras perdidas que durante la exposición se pudieron ver inicialmente como responsabilidades propias del área de Ti, sin embargo, fuimos aclarando el alcance y la cobertura del área de tecnología y su relación con dicho riesgo. Indudablemente las tareas complejas están bajo su resorte, es decir, bajo su tutela y son ellos los llamados a responder por las mismas, sin duda alguna, pero aquí entran a jugar un nuevo concepto directamente ligado a la responsabilidad y es "La culpabilidad" la cual tiene dos acepciones denominada la primera como, responsabilidad sin representación que conduce únicamente a "Sanciones" por los incumplimientos directos de las responsabilidades y la con representación, que puede conducir a castigos más severos e inclusive con la detención, por las pérdidas incurridas a los bienes patrimoniales!

¡Una vez explorado todo ese largo camino de la responsabilidad versus la culpabilidad, comprendiendo su relación, se describen las recomendaciones o principios básicos a tener en cuenta por la Junta Corporativa a fin de demostrar con suficiencia su gestionar de cara al tratamiento del Riesgo Cibernético y explicando de forma somera uno a uno cada principio. El primero nos lleva a comprender que la gestión del Riesgo Cibernético no es tan solo una responsabilidad exclusiva del área de TI, sino que por el contrario y con una visión más global, debe tratarse como una responsabilidad interdepartamental. El segundo demostró que la Junta Corporativa puede tener efectos legales por el incumplimiento de sus funciones. El tercero a mi criterio es el más importante dado que fija algunas pautas mínimas requeridas para justificar con evidencias objetivas la gestión de la Junta Corporativa respecto al conocimiento, tratamiento y accionar frente al Riesgo Cibernético. El cuarto principio enfoca a la junta a entender la gestión del riesgo no, como una carga empresarial y un nuevo centro de costo, sino por el contrario entenderlo como un elemento estructural de la gestión global que deja más beneficios que cargas. Finalmente el quinto refuerza la idea, que una buena gestión del riesgo, con independencia de su origen, refuerza el proceso de toma de decisiones a fin de poder establecer con precisión que apetito al riesgo se quiere moldear en la entidad.

¡Aunque el inicio fue abrupto y para algunos casos en los participantes de la cátedra fue molesto por la descripción de las características de la Junta Corporativa, la motivación intrínseca era moverlos y llevarlos a escenarios poco cómodos e intolerantes, para que puedan hacer un buen proceso de auto-reflexión y autocritica de sus casos particulares. Nunca fue mi intensión ofender a nadie, pero si propiciar al autocontrol. Considero para tranquilidad del curso, que para entender la importancia de la Junta Corporativa es necesario ver la siguiente analogía; cuando vamos todos en un gran bus bajando el despeñadero de una montaña pero el bus no lleva conductor, significa que existe mucha probabilidad que se materialice un accidente, pero si por el contrario tenemos abordo como conductor un estamento conformado por varios conductores, todos expertos en diferentes aspectos del transporte, es decir, control de velocidad según estado de la vía, estado material del mantenimiento del motor, conductor de reemplazo entre otros, la probabilidad de tener un accidente es muy, pero muy baja.!

Pese a todo…!los espero en la próxima clase!