GOBIERNO DE LA CIBERSEGURIDAD

ROBERTO BARATTA MARTÍNEZ

La primera disyuntiva, habitual en entornos complejos y tan cambiantes como el digital, máxime en un momento de absoluta inmersión no ya de los sistemas económicos, de mercado, administración y sociales si no ya en la vida cotidiana y personal de cualquier individuo, es «saber de qué estamos hablando». Y en el mundo empresarial este entendimiento es especialmente sensible y está siendo un camino complejo y atiborrado de conceptos dispares que no siempre ayudan.

INTRODUCCIÓN

La Ciberseguridad como término tiene relativamente poco tiempo de vida. «Ciber-» es un término acuñado por la RAE como «relación con redes informáticas» por lo que extendiendo esta definición hablaríamos de «seguridad relacionada con redes informáticas». Una definición algo pobre para la relevancia que ha adquirido del concepto.

Digamos que de forma extensiva Ciberseguridad aparece con la necesidad de proteger los sistemas informáticos de las empresas de ataques maliciosos que afecten a su correcto funcionamiento y ocasionen daños. Sería una parte de la tradicional Seguridad Informatica o Seguridad de la Información más clásica.

Extendiéndolo a la vida cotidiana, ya que los sistemas informáticos ya forman parte de nuestro devenir diario (tenemos tanta capacidad informática en el bolsillo, si no más, que en el equipo de mesa o de trabajo) y el perímetro entre perfil personal y profesional se ha diluido completamente.

Hablamos por tanto, del Gobierno de la protección de los sistemas informáticos de una empresa u organización ante cualquier disrupción, afectación o alteración, especialmente aquellas intencionadas, maliciosas y dañinas. Nada menos.

Gobierno

Cuando hablamos de Gobierno se nos antoja un término de amplia complejidad que puede ser entendido de múltiples formas. Y así es en lo lingüístico y lexicográfico. Pero al fin y al cabo no es más que la función, proceso y procedimiento de gestionar algo.

El gran reto está siendo, y será, incorporar a los niveles de decisión de una organización una función que ha sido eminentemente técnica, relacionada con la tecnología y las comunicaciones, que ya de por si suponen un problema reflejar en términos de negocio y gestión expresiones operativas que no siempre tienen una fácil descripción de gestión.

La tecnología se enfrenta al reto de su propia «*comoditizacion*», con la licencia del término, lo cual significa que la extrema complejidad de lo digital se aplica a la vida cotidiana de individuos y organizaciones de forma absolutamente relacionada, integrada, necesaria e imprescindible. Nadie espera que su teléfono móvil no funcione o se conecta cada mañana. Igual que esperamos que haya agua corriente o electricidad disponible.

Si a este reto de convivencia tecnológica le aplicamos la necesidad de la confianza y resiliencia de estos sistemas, nos encontramos en un nivel de expectativas donde aparece la sombría figura del uso ilegitimo, la vulneración, disrupción y demás maldades inherentes al uso masivo, democrático y global de la tecnología.

Y donde era suficiente en el pasado con garantizar la continuidad y recuperación de los sistemas, cierta capacidad de autenticación y acceso y control del flujo de información; nos encontramos ahora que debemos discernir que uso es legítimo y adecuado, garantizar la operación incluso en los peores escenarios y cumplir regulaciones garantistas al nivel de la propia individualización del uso digital y de la relación con nuestro entorno.

Es precisamente el entorno, la esencia misma de la interrelación por medios digitales con nuestros par, igual, administración y compañías lo que fuerza y a la fuerza requiere un alto grado de confiabilidad. No solo ya por la obvia necesidad de garantizar que los servicios digitales se prestan a quien los requiere en tiempo y forma (todo tiempo y todo lugar prácticamente) si no que se hace en virtud de las características sociales, legislativas, éticas y estéticas oportunas. Cuando es ya cosa de todos, es objeto de reflejo de lo mejor y de lo peor de la esencia humana, y por lo tanto debe ser objeto de regulación y control.

La famosa transformación digital, como si hubiera una nueva, como si no estuviésemos constantemente inmersos en ella desde hace años y años, quizás como humanos desde siempre, transforma a velocidades de vértigo la forma de hacer. Los individuos nos hemos transformado solos, no hemos necesitado que nos indiquen, maticen o elaboren planes para nuestra transformación digital.

Quizás por primera vez estamos ante un escenario en donde la innovación, usos y transformación parten de los propios individuos, de los usuarios donde tenemos la masiva capacidad de impulsar formas y usos y denostar otros. Simplemente porque podemos.

Tradicionalmente la tecnología se ponía a disposición de los individuos, e incluyo a las organizaciones, en una ruta marcada de investigación y desarrollo, patentes e industrialización, comercialización y producción, despliegue de servicios y uso y consumo. Es decir, llegaban los servicios tecnológicos a los ciudadanos, especialmente los prestados por organizaciones, en una aproximación «*top-down*» que requería sus pasos y sus tiempos.

Hoy, la «gente» utiliza la tecnología de formas sorprendentes, produce sus propios servicios digitales, los consume como le place y exige a las organizaciones y fabricantes usos no pensados o diseñados previamente. Decide y consume tecnología como nunca. Arbitrando un escenario donde no hay nada preestablecido y todo puede ser reutilizado de formas absolutamente innovadoras y maravillosas, fuera de laboratorios y universidades. La «digitalización de la calle».

Y esto está al alcance de cualquiera. Tanto para producir y enriquecer como para explotar, malversar y delinquir. La *comoditizacion*, democratización y globalización es lo que tiene. Hay para todos.

La exposición a daños, disrupciones, alteraciones y usos indebidos de los sistemas de información y comunicaciones, de los datos la tecnología que los sustenta y los procesos en que están implicados siempre han formado parte del interés de las organizaciones. La diferencia es la cantidad, calidad y escenarios a los que nos enfrentamos hoy. La multiplicación de la dependencia de la tecnología, los usos sociales, la interrelación con administraciones y otras organizaciones ofrecen un escenario donde la reflexión y pensarse las cosas de nuevo es más que necesario.

Intentemos aquí diseñar un acercamiento a la Ciberseguridad en doble sentido, de abajo arriba, partiendo de una aproximación más técnica y tecnológica, más ingenieril, hasta llegar a los niveles de gestión y gobierno de una organización. Y al mismo tiempo de arriba abajo, desde la perspectiva de la gestión empresarial, de la visión de los que deben tomar decisiones y estrategias, bajando hasta identificar qué y cómo soportar esas decisiones en el día a día, en la operación y en la planificación. Veamos cómo.

DEL ACTIVO AL PROCESO

En una aproximación de abajo a arriba en la organización, corresponde en primer lugar disponer de un inventariado y clasificación de activos tecnológicos y de información adecuados. Ahí es nada.

En una organización de tamaño acotado o de muy reciente establecimiento, puede considerar algo asumible y no muy complicado disponer de un sistema similar, del tipo de las tradicionales CMDB (1) o similar. En una organización compleja y de tamaño relevante, que además tenga ya a su cargo sistemas de años, producto de múltiples cambios, de crecimientos o recortes, de fusiones, de integraciones etc. puede ser una auténtica pesadilla. Pero es necesario conocer que tenemos para decidir cómo protegemos (y que protegemos) contra que y por qué.

Entonces podemos concluir que en esta aproximación, lo primero que tenemos que determinar es el correcto gobierno de los activos de información y tecnología, empezando por su inventariado y clasificación. Y este puede y debe realizarse desde distintas ópticas: técnica (servidor, base de datos, Smartphone….), de servicio

FIGURA 1

2

Fuente: Elaboración propia

FIGURA 2

Fuente: Elaboración propia

(correo electrónico, almacenamiento, internet…), de negocio (nomina, facturación…) de canal (TPV, Marketplace….) estratégico incluso (ventas, servicios, marketing…). (2)

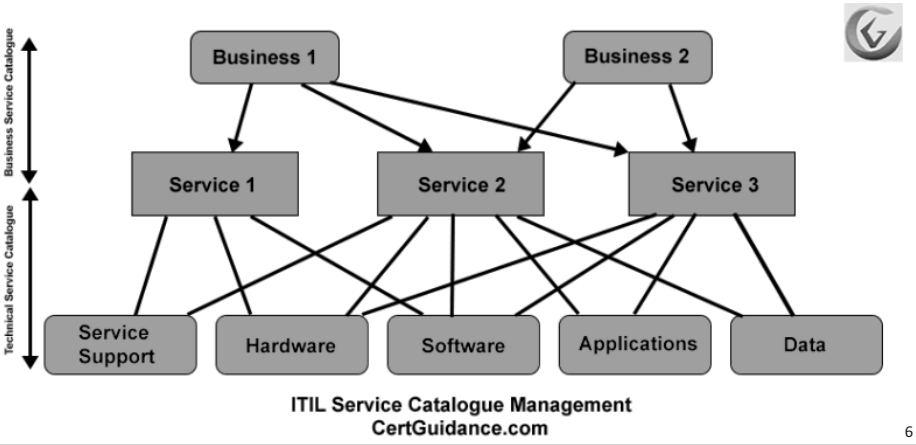
No es el alcance de este texto evaluar mecanismos y aproximaciones al gobierno de la Tecnología y los Sistemas de Información. Hay suficientes marcos, metodologías y aproximaciones para poder afrontarlo con la soltura necesaria para aportar en la aproximación «*bottom-up*» a la gestión de la Ciberseguridad. Pero en cualquier caso, es una cuestión de «vuelta a lo básico». A establecer los mecanismos adecuados para determinar un inventario detallado, preciso, actualizado y gestionable de todos y cada uno de los activos tecnológicos de una organización. Nada más y nada menos, tarea ímproba en sí misma.

Sea cual sea la taxonomía utilizada para su identificación, la función de Tecnología en una organización debe ser informada y reconocer la relevancia que el inventario tiene para el aseguramiento y por tanto la Ciberseguridad. Parece evidente pero puede no serlo. Incluso aproximaciones dispares pueden tener resultados complejos o complejos de gestionar. Por ejemplo, un activo «servidor» puede ser demasiado amplio y ser más relevante dividirlo en «servidor Windows», «servidor Linux»…. Desde el punto de vista de Ciberseguridad seguro es relevante.

Y si el trabajo de disponer de ese inventario ya es un reto en sí mismo, aplicar sobre los activos incluidos (debemos suponer que todos los existentes….) las guías base de seguridad necesarias. Es decir, hay que determinar, evaluar en función de riesgo y amenazas, consensuar con los dueños de esos activos el cómo aplicarlas, aprobarlas formalmente, hacer seguimiento e identificar debilidades de aplicación y gestionarlas. Tenemos entonces el primer escalón de la Gestión de la Ciberseguridad en esta aproximación de abajo a arriba: la seguridad de los activos. (3)

Suponiendo tenemos ya los activos de tecnología identificados, gestionados y securizados (4) (o asegurados) según se determina en la organización, el siguiente paso es hacernos una pregunta muy sencilla de respuesta muy compleja: ¿una brecha o incidente de seguridad en este activo que supone para la organización?

FIGURA 3



Fuente: Elaboración propia

Lo más probable es que la respuesta a esta cuestión seria de tal alcance y matices que no se podría gobernar una aproximación tan variable y amplia. Por ejemplo, ¿Qué supondría que una vulnerabilidad de una estación de trabajo de un departamento o unidad fuera explotada por un malware que instalara *Ransomware* (5)? Pues depende. De si se extiende, de si ese activo es el único, si ese activo es de un administrador, si lo es de una aplicación critica, como impacta en negocio, si implica infringir alguna regulación interna o externa, etc., etc.

Por lo tanto es muy recomendable elevar a un nivel superior la identificación de los activos para tratar de obtener una visión agregada.

ACTIVO, SERVICIO Y PROCESO

Una aproximación muy útil puede ser asociar los activos a los servicios tecnológicos que se prestan en la organización. Este concepto es amplio también y debe determinarse a que corresponde y como. Pero básicamente se trata de basarse en el portfolio de Tecnología. (6)

De este modo, un conjunto identificado de activo de bajo nivel (servidor, base de datos, aplicación….) estará asociado a un servicio de IT (correo, navegación, desarrollo de software, mantenimiento de sistemas…) y este soporta procesos de negocio identificados en un Mapa de Procesos. Con este flujo de abstracción del detalle a la generalidad se consiguen varios objetivos:

1. Contemplar el detalle como un todo, agregando los riesgos de bajo nivel a procesos de negocio de alto nivel

2. Asociar activos concretos a «lo que realmente importa» que son los Procesos de Negocio. Que a su vez se habrán priorizado según la estrategia de la organización.

3. A pesar de abstraer, el concepto de «servicio de TI» permanece a un nivel suficientemente técnico y con una estructura tecnológica definida que permita aplicar marcos de control de Ciberseguridad. Por ejemplo, desde el parcheado de equipos y su bastionado, hasta el «*threath hunting*» (7) avanzado pasando por detección de comportamiento y «*machine learning*».

A su vez comporta una serie de dificultades no desdeñables.

1. La correcta identificación de activos. ¿Son todos los que están? ¿están todos los que son? Es en sí misma una tarea compleja pero que cualquier organización de TI debe cometer: conocer su instalación de forma actualizada.

2. Abstraer riesgos concretos (por ejemplo, vulnerabilidad critica en un servidos de base de datos no «*parcheable*» por impactos en la aplicación) a un servicio de TI y a su vez un Proceso. ¿Hay controles compensatorios? ¿Plan de acción?

3. Por supuesto, la gestión por Procesos. No todas las organizaciones se gestionan de esta manera, y las que lo hacen asumen un importante reto. Es posible quedarse en el nivel servicio TI, aseguraría la primera línea de gobierno relativa a conocer las operaciones y como se sustentan. Quedaría más coja la aportación de valor real a negocio pero es algo que se puede gestionar y trabajar con las unidades de negocio, organización o similares. Imaginación al poder.

Llegado este punto, donde ya disponemos de un inventario aceptable, reconocible y gestionable de activos; una descripción de «servicios TI» que se prestan a la organización o directamente a clientes o terceros; y una asignación adecuada de cada activo a ese servicio, hemos levantado una información y una forma de gestión tecnológica (aun no hablamos de Ciberseguridad) que en si misma ya es un importante logro. Y tan complejo es levantarlo como para que por inadecuada

FIGURA 4

Fuente: Elaboración propia

gestión y deficiente procedimiento se degrade, que lo hará y rápidamente. Por tanto es realmente significativo cuan de relevante es el Gobierno de la Tecnología para el Gobierno de la Ciberseguridad.

En este ya prometedor estadio, donde la iniciativa, por qué no, de Ciberseguridad ha llevado a Tecnología a «ordenarse más y mejor», es cuando comienza el trabajo de estimación, identificación y detalle. Estimación es identificar el mapa de amenazas para nuestros activos, y por tanto para los Servicios TI. ¿Es la ex filtración una amenaza relevante en los servidores de correo? pongamos como ejemplo; claramente si, la información que alojan es más que relevante.

Identificación seria el trabajo específico de valorar esa amenaza, en el ejemplo, tipo de conexión al exterior del correo, filtros y controles aplicados, etc.

Y el detalle es finalmente cuantificar el riesgo residual, si lo hay, su nivel de relevancia y el plan de acción al respecto.

Esto no suena a todos: metodología de análisis de riesgos. Tal cual. Algo que de forma natural se realiza en cualquier competencia de Ciberseguridad pero que muchas veces no está normalizado y lo que es más relevante y afecta directamente a la función de Gobierno: publicado, aprobado y comunicado a quien deba estar informado y tenga capacidad de decisión. (8)

Sobre esto volveremos porque en sí mismo es una de las funciones más relevantes del Gobierno de la Ciberseguridad: promover las discusiones oportunas en base a la información adecuada para alimentar una toma de decisiones correcta.

Sobre unos activos con su análisis de riesgo realizado e identificado, abstraído ese riesgo a los servicios que apoyan esos activos, no debería ser muy complicado identificar los procesos de negocio o similares a los que sustentan o apoyan. En el ejemplo del correo electrónico anterior: unos activos (servidores) expuestos a una amenaza (ex filtración) que puede ser explotada por una vulnerabilidad (falta de parcheado) resulta en un riesgo alto en el servicio de correo electrónico que presta TI a toda la organización. Y podemos fácilmente comprobar como el proceso de contratación (por ejemplo) utiliza masivamente el correo electrónico y por tanto ese Proceso de Negocio soporta un riesgo alto.

Suponiendo que ese Proceso de Contratación es relevante para la compañía, ¿no correspondería explicar en los órganos de decisión de la compañía que tal proceso clave tiene un riesgo alto de Ciberseguridad y porque? ¿Con que objeto? Pues probablemente conseguir al menos la aprobación de presupuesto o recursos urgentes para acometer el correcto parcheado de esos equipos, o sustituirlos. Y en el peor de los casos, que la dirección conozca los riesgos y pueda tomar la decisión de incluso aceptarlo, si la evaluación de costes o la oportunidad por ejemplo no es la adecuada, de transferirlo externalizando el servicio de correo, contratando una ciber póliza, etc.

Acabamos de realizar en pocos párrafos un magnifico ejercicio de Gobierno de la Ciberseguridad. Fácil de escribir pero no tan fácil de aterrizar. Pero tener un objetivo es el primer paso de un plan.

DEL NEGOCIO A LA TECNOLOGÍA

Volviendo al inicio de este artículo, en contraposición al análisis de abajo a arriba realizado, tenemos otro enfoque diferente, compatible y simultaneo si se desea. E incluso, como veremos, incluso sustitutivo uno del otro.

Un acercamiento también interesante es la identificación de «que es relevante para la organización» a alto nivel. Esta identificación debe ser siempre promovida por los niveles de decisión mayores de la compañía u organización. Esta intrínsecamente ligada a la estrategia y por tanto a la propiedad (accionista en su caso), a la dirección y planificación estratégica, a la responsabilidad corporativa y cualquier otro elemento de relevancia en la decisión de mayor nivel jerárquico.

«Que es relevante para la organización» puede concluirse con un mayor o menor nivel de detalle. Cosa importante a la hora de aterrizar una ruta táctica desde la estrategia. Conclusiones del tipo «ser líder en el sector», «ofrecer la mejor experiencia a nuestros clientes», «aumentar la facturación en el segmento X» o «reducir los fondos ajenos en un %» no parecen ayudar mucho.

Obviamente es de suponer que esas líneas estratégicas van acompañadas con planes más detallados que si nos proporcionaran mayor información. «Ser líder en el sector» podría acompañarse de «abrir más delegaciones», «contratar X personal», «aumentar la facturación», «fomentar canales alternativos»…que ya pueden alinearse más con la identificación de relevancia para la compañía.

¿Dónde obtener la información necesaria para iniciar este camino «*top-down*» de forma adecuada y con la

adecuada retroalimentación y actualización? Pues si el camino es desde «arriba» será en los más altos círculos de decisión de la compañía u organización donde obtener esta información. Esto nos lleva necesariamente a una reclamación clásica «presencia y visibilidad en la alta dirección», un «mantra» cotidiano y continuo en la función de Ciberseguridad, adolecida por una historia vinculada al ostracismo técnico y a un virtuosismo informático, poco entendido y menos valorado clásicamente en la organización.

Pero, ¿cómo lograr esa posición que permite a la Ciberseguridad auparse en jerarquía organizativa que aporte la necesaria visibilidad para no ya participar del diseño y de la estrategia, si no al menos tener la información necesaria para elaborar una aproximación que aporte valor? Desde luego es parte fundamental del Gobierno de la Ciberseguridad el modelo organizativo.

Dependiendo del tamaño, estructura, ámbito y negocio, cada organización tendrá que desarrollar una estructura donde la Ciberseguridad desempeñe sus funciones. Pero lo primero será definir cuáles son. Veamos como:

- Misión: es el motivo o razón de ser de la función de Ciberseguridad. Está vinculada al presente a lo que se espera y como se desempeña. Será necesario definir una «misión» de la función, alineada con la visión estratégica ya que depende de la función y objetivos de la compañía, pero en el caso de la Ciberseguridad con ente propio y donde se recoja el espíritu y forma de la función en la compañía. Un ejemplo: «desarrollar capacidades de protección y respuesta ante amenazas cibernéticas para la protección de la compañía y sus activos»

- Visión: es el objetico que queremos lograr. De igual forma, debe ser definido correctamente para la función. Como ejemplo: «aportar valor tangible a la organización reduciendo los riesgos de Ciberseguridad y apoyando las operaciones». Está vinculada a la organización y capacidades que deben conducir al objetivo.

- Estructura: la definición de misión y visión nos guía a determinar una organización adecuada para responder a lo que se espera de la función (misión) y a lo que debe aspirar (visión). Para ello debemos responder a cuestiones como:

    - ¿Quién desempeña la misión? Estructura organizativa. ¿dentro de tecnología? ¿de operaciones? ¿de control?....

    - ¿Quién asume el rol y por tanto la responsabilidad? ¿Existe la figura del CISO (Chief Information Securty Officer (9)) o similar? ¿Qué dependencia orgánica ay funcional tiene? (frente a quien responde).

    - ¿Quién supervisa la función y quien es informado sobre la misma? ¿existe una estructura de rendimiento de cuentas e información? ¿formal o informal? ¿existe una función auditora de Ciberseguridad?

    - ¿Tiene claramente definidas la función sus roles y responsabilidades? ¿están entendidas y reconocidas por la organización?

- Modelos y marcos de gestión: llegados a este punto, donde la misión y visión han sido establecidas y se dispone de una estructura de gestión llega el momento del «como». Es necesario definir un modelo de gestión de Ciberseguridad, normalmente basado en alguno de tantos existentes (COBIT, NIST…). El marco elegido, o bien desarrollado internamente si es el caso, no muy recomendable ya que el esfuerzo será grande y será muy difícil la comparación y *benchmark* (10) a futuro; debe acompasar la estrategia, capacidades y objetivos y no convertirse en un fin en sí mismo sino en el medio para.

  No es el objeto de este articulo le identificación de los marcos existentes y sus bondades y complejidades. Hay suficiente literatura al respecto y en este texto simplemente se pretende despertar la inquietud y servir de guía inicial para el gobierno de una función relativamente nueva, compleja en sí mismo y que requiere liderazgo para su desarrollo y reconocimiento en las organizaciones. Es decir, el sendero a transitar esta delante y es responsabilidad de los profesionales de la Ciberseguridad echar a andar y abrir camino.

- Recursos y presupuestos: y obviamente llegamos al momento de «con qué». Disponer de un presupuesto y recursos suficientes para, en base al marco definido, lograr los objetivos propuestos, es una parte más de la gobernanza de la cosa. Evaluar las necesidades y determinar un presupuesto no es nada sencillo. Pero es un trabajo necesario y que debe incluir el detalle de que, por qué y para qué. Que se necesita, por qué se necesita y que objetivo alcanzaremos con ello. Un «caso de negocio» al uso.

Llegados a este punto nos encontramos con la necesidad de cuantificar una aportación de valor real de la Ciberseguridad a la organización. De construir un «*caso de negocio*» donde la inversión a efectuar reclame unos resultados adecuados, entendibles, medibles y repetibles. Y no es cosa sencilla.

Una aproximación clásica de la Ciberseguridad siempre ha sido proteger, con otros alcances pero básicamente proteger. Pero, ¿proteger qué? Proteger todo, ¿acaso todos los activos de información, la tecnología que los sustenta y los procesos que los explotan no deben ser todos y cada uno protegidos? Este discurso tuvo y tiene aún su espacio. Lo primero es determinar como vimos la visión y misión en base a la organización y su estrategia. No es lo mismo que la organización sea una agencia militar responsable de fuerzas de ataque, que una entidad financiera, un ministerio, una central nuclear o una tienda online.

Protegerlo todo nos lleva a una constante necesidad de inversión y esfuerzo que no necesariamente conlle-

van mejoras niveles de Ciberseguridad, mejor entendimiento en la compañía y lo que es peor, aportación de valor real, esencia de cualquier función corporativa. Alguna vez nos puede llevar la tentación de creer que seguridad (ciber en este caso) es lo primero, pero intentar siquiera evaluar responder a la pregunta de que es primero, si los objetivos de seguridad o los de negocio, es que aún no lo hemos entendido.

Volviendo al caso de negocio, es obvio que trabajar en reducir los riesgos, en evitar incidentes y en protegernos de futuras amenazas entra de lleno en el mundo de la adivinación y casi del esoterismo. Identificar qué es lo más relevante para la organización, evaluar las amenazas en base a estadística y prospección, aplicar criterio experto y benchmarking, definir tolerancia al riesgo y trabajar en aceptarlo, mitigarlo o transferirlo no es exclusivo de Ciberseguridad. Es más, es una ruta incluso algo ajena en modo formal a la tradicional gestión. Pero casi todo está escrito, por lo que encontrar el mecanismo de evaluación de riesgos que nos lleva a determinar que una inversión nos ayudara a reducir riesgo no debería ser muy complejo.

Pero además, la inversión ciber proporciona en muchas ocasiones sinergias y eficiencias no tan obvias como las de riesgos pero muy útiles y provechosas. La gestión de volúmenes importantes de información puede proporcionar mejoras de la eficiencia (por ejemplo la gestión de identidades centralizada no solo reduce riesgos de integridad y confidencialidad si no que permite provisionar y mantener usuarios de forma eficiente y veloz, reduciendo tiempos), puede aportar visiones totalmente nuevas de la información (otro ejemplo, la monitorización de dispositivos móviles puede darnos pautas de uso que permitan optimizar tareas comerciales o de atención a clientes), e incluso proporcionar información de negocio inédita (por ejemplo, hábitos y costumbres de los clientes en base a la monitorización de su actividad y predicción).

Construir un caso de negocio donde «las cuentas den» no es fácil pero debería ser una tarea obligada en cualquier inversión en Ciberseguridad (o en cualquier otra). Existen mecanismos varios para estimar los impactos de materialización de riesgos, pero también deben considerarse otros ahorros e incrementos valiosos y para ello es necesario tener una visión global, pedir ayuda a potras unidades y visión «desde fuera», evitar que los arboles nos dejen ver el bosque. Esta práctica además permite una mejor interacción y entendimiento con las áreas financieras y de compras, que tendrán más sencillo valorar los recursos y presupuestos asignados a la función; por las áreas de negocio que entenderán mejor los objetivos y en que les afectan, y en las de control que tendrán una visión más sencilla para determinar qué se está trabajando en lo importante. Y lo que es mejor de todo, la propiedad, alta dirección o niveles de decisión de la organización entenderán las propuestas, el valor esperado y por tanto la relevancia, visibilidad e influencia de la función. Que es el objetivo básico por el que comenzamos párrafos arriba.

Pero nos quedaría un aspecto si cabe tan relevante: las personas (11). Toda organización la componen personas que, por mucha tecnología que aportemos y por muchos escenarios complejos diseñemos, son las que marcan la diferencia. Está demostrado (12) que el factor humano es clave en el entorno digital actual, tanto como rigen de las brechas de seguridad donde estudios afirman que hasta un 35% son producidas por errores o negligencia humana: como en la primeria línea de defensa ciber.

A pesar de que la tecnología suple y suplirá a los humanos en muchas facetas, lo que se ha puesto de manifiesto en la explosión tecnológica delos últimos años es que al aportación humana es clave y que la tecnología apoyara radicalmente la visión humana, pero difícilmente la sustituirá. Y por tanto, siendo las personas el activo más valioso de cualquier compañía, dotarse de los perfiles adecuados en Ciberseguridad será clave para el éxito.

El mercado adolece de profesionales cualificados (13), y el escenario no parece mejorar en un futuro cercano. Identificar los profesionales adecuados puede ser una tarea ímproba. Es una buena aproximación buscar talento interno, aunque no especializado si adaptable, además de las oportunidades externas. Es relevante capacitar constantemente no solo ya al personal de la función si no a otras unidades relevantes como Tecnología, Recursos Humanos, Financiera e incluso Comercial. La Ciberseguridad es cosa de todos, en el ámbito personal y profesional por lo que la preparación y concienciación siempre serán un activo valioso.

La organización de la función dictara el tipo de perfil necesario, básicamente técnico y entrenado pero no solo. Cada vez es más relevante el conocimiento de analítica de datos, de algorítmica y matemática, de legal y contractual…en una función amplia estos perfiles tienen no solo espacio si no mucha relevancia.

GOBERNANZA

Llegados a este punto donde disponemos de una estrategia (misión y visión), de una organización y de unos medios; toca gestionar el día a día aplicando nuestro marco de gestión, nuestras metodologías y demás.

Toca desempeñar las funciones encomendadas, toca gestionar los riesgos, los presupuestos, las personas…. Y para ello es necesario desarrollar modelos de medición, de información y de seguimiento adecuados. Es necesario identificar métricas e indicadores, en base a los objetivos de medición (KPI, KRI, KCI…) que nos permitan acreditar el correcto desempeño de las funciones, estimar los riesgos y sus impactos y dar probada muestra de ello a la organización además de proporcionar información de valor y relevante para la toma de decisiones.

Hablamos por tanto, de la Gobernanza de la Ciberseguridad o lo que es lo mismo según la RAE (14) «arte o manera de gobernar». Veamos por donde comenzar.

FIGURA 5

1

Fuente: Elaboración propia

Desempeño: Resultado de ejercer las obligaciones inherentes a la función. Por lo tanto debe ser identificable, medible y repetible. Un indicador de desempeño (o KPI) proporcionara información del nivel de resultados, de alcance de una acción o función. Un ejemplo podría ser «% *usuarios formados en Ciberseguridad*». Pero también objetivos más de gestión como el seguimiento presupuestario u horas dedicadas por proyecto.

Nivel de riesgo: identificación de exposición al riesgo en forma medible (o KRI) que permita realizar un seguimiento y que proporcione mecanismos de alerta temprana. Un ejemplo: % vulnerabilidades críticas en los sistemas. O también elementos cuantitativos como «*perdida por fraude online*».

Es interesante observar como un KPI y un KRI se relacionan entre sí, donde un KPI determina alcance, un KRI puede determinar riesgo, en el ejemplo anterior: «% *usuarios formados en Ciberseguridad*» puede ser un indicador de desempeño de una campaña de formación siendo al mismo tiempo y con un leve cambio un indicador de riesgo «% *usuarios NO formados en Ciberseguridad*» que determine cuan expuesto está el personal a fallos relacionados con la Ciberseguridad. (15)

Este mecanismo de medición e informes debe tener su propio objetivo en función de la estrategia para proporcionar información de seguimiento y toma de decisiones, por tanto, deben consolidarse en un «cuadro de mandos» adecuado e integrado que permita diseñar un Sistema de Gestión de la Seguridad de la Información o SGSI.

Existen múltiples descripciones de un SGSI pero la mejor aproximación sería la de la norma ISO que la desarrolla, la ISO 27001 (16): «*un proceso sistemático, documentado y conocido por toda la organización*» que es básicamente lo que llevamos describiendo en este artículo.

Podemos, reduciendo mucho el alcance al objeto de ser más didácticos y explicativos, entender el Gobierno de la Ciberseguridad como «*el conjunto de las prácticas y responsabilidades ejercidas por la dirección y ejecutivos de una organización al objeto de proporcionar visión estratégica para el logro de objetivos asegurando la gestión apropiada de los riesgos de Ciberseguridad con los recursos adecuados.*» (17)

El componente adicional a la estructura de Gobierno de Ciberseguridad sería la propia aportación de valor que podría, y debería, desglosarse en valor propio esperado de la función y valor añadido o agregado, muy relacionado con la visión y misión pero también con el acercamiento a negocio y la capacidad, incluso imaginativa, de evaluar esa aportación. Pero vayamos primero con lo más básico identificando los beneficios de la propia función como son:

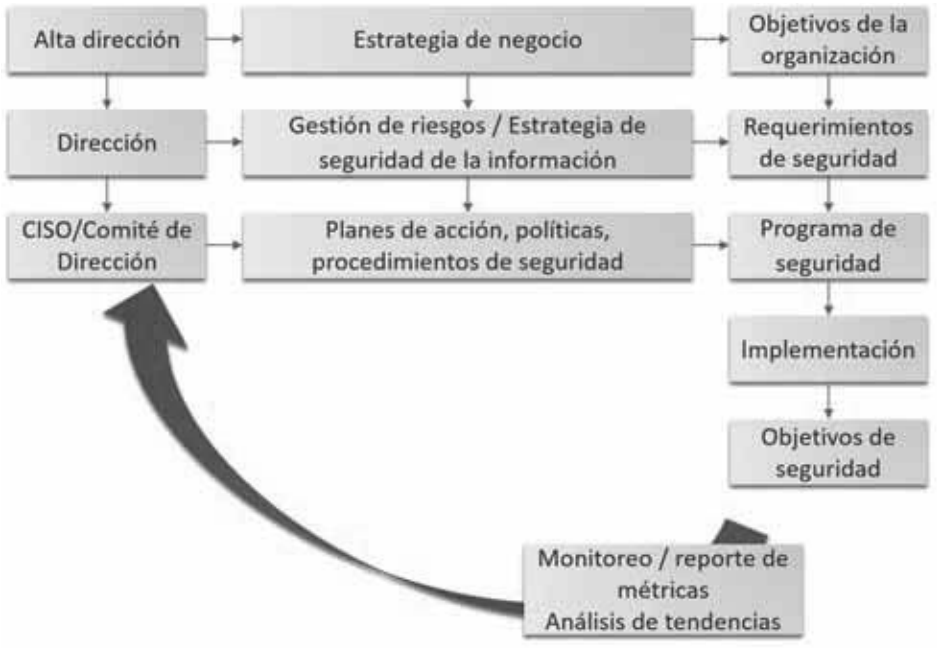
- Mejorar la confianza en las relaciones con los clientes.
- Proteger la reputación de la organización.
- Reducir la probabilidad de violaciones de privacidad y sus sanciones y responsabilidades.
- Proporcionar mayor confianza en las interacciones con terceros.
- Permitir nuevas y mejoradas capacidades digitales, incluyendo las transacciones electrónicas.
- Reducir costes operativos mejorando los riesgos que afectan a los procesos con resultados predecibles.

Entendemos estos beneficios como propios e inherentes a la función de Ciberseguridad en una compañía, compartidos en gran medida con la Seguridad de la Información más clásica pero indesligable del todo de la Ciberseguridad. En sí mismos, suponen ya una aportación fundamental y valiosísima para cualquier organización actual, máxime en aquellas de «base tecnológica» (18), que «*basan su actividad empresarial en la innovación tecnológica orientada al mercado, dedicándose a la comercialización y rentabilización de productos y servicios innovadores generados a partir de un uso intensivo del conocimiento científico y tecnológico, y que cuentan con personal investigador y técnico de alta cualificación en sus equipos*».

Esta definición aplica también a las empresas que de forma masiva utilizan tecnología y canales digitales como modelo de producción y entrega de servicios. Básicamente compañías del sector servicios como el financiero, telecomunicaciones, etc. y al que se está incorporando de forma muy acelerada la administración pública.

Pero no podemos obviar la aportación de valor añadido, lo que está por encima de las expectativas de la función y sus objetivos iniciales pero puede constituir en sí mismo un valioso instrumento de éxito en la organización. Hablamos de lograr aportaciones de valor mientras se alcanzan los objetivos previstos. De poco valdría proporcionar valor añadido si el valor esperado no se alcanza. Primero la función y sus objetivos, sean lo ambiciosos que sean, luego viene el resto, eso sería un go-

FIGURA 6



17

Fuente: Elaboración propia

bierno adecuado, ver descripción más arriba: «…*para el logro de objetivos…*».

Veamos en que escenarios la Ciberseguridad puede generar valor más allá de los objetivos específicos:

- Cumplimiento: el cada vez más complejo escenario de regulación, donde a las normativas sectoriales o de mercados se le unen nuevas directrices gubernamentales, transnacionales e incluso globales, además de buenas prácticas o estándares de la industria, requiere de un nivel de controles y monitorización de los mismos, además de seguimiento de operaciones, comportamiento t flujos de información que caen completa o en parte en las competencias de Ciberseguridad. Muchas veces los controles y funciones ya existentes en una compañía, enfocado adecuadamente pueden proporcionar de forma eficiente (evitando en muchos casos nuevas inversiones y esfuerzos considerables) el alcance de cumplimiento necesario. Una adecuada relación con los responsables de cumplimiento con un buen entendimiento del mismo y de las necesidades de la organización pueden determinar que el programa de Ciberseguridad de una compañía u organización apoya, promueve y facilita la estructura de cumplimiento necesaria.

- Valoración de negocio o «Business Valuation»: más allá de los impactos tecnológico, de operaciones e incluso legales esta la reputación de una entidad. Esta reputación maraca en muchos casos le estimación del valor de una compañía ara su propiedad, los accionistas, el mercado… Esta reputación es un activo complejo en su valoración y evaluación pero la Ciberseguridad puede y debe contribuir de forma definitiva a proteger run activo tan relevante. Incluso la valoración de las capacidades de ciber- resiliencia están comenzado a ser relevantes en la valoración de una compañía. (19)

- Cadena de suministro: es obvio que la necesidad de disponer de un marco de control interno en todos los sentidos necesarios de la organización., incluyendo la Ciberseguridad, es una necesidad. Y en un mundo hiper conectado donde el ecosistema de funcionamiento de cada organización es cada día más complejo, este marco de control debe garantizar la inclusión de aquellas terceras partes que participan de forma relevante en el negocio y sus procesos. Y por tanto, extender el marco de control a los proveedores y otros actores es fundamental, incluyendo por tanto en las evaluaciones, contratos, licitaciones y relaciones con terceros las consideraciones en materia de Ciberseguridad que se consideren.

- Ingeniería de la información y análisis de datos: la propia naturaleza de las funciones de Ciberseguridad implican la recopilación, tratamiento, evaluación y consolidación de información de todo tipo. Además en tiempo real o casi real. Esta información seguro incluye datos de negocio, de clientes, de empleados, de los sistemas… información que tratada de forma adicional a la de su función base puede proporcionar información muy valiosa a las unidades de negocio a la que puede no tengan acceso o simplemente nunca se les había ocurrido pedir o preguntar. La monitorización de usuario per-

mito conocer las prácticas habituales en una organización, seguro que relevante para Recursos Humanos o incluso para Operaciones, o Comercial. La de dispositivos y activos tecnológicos conocer el grado de uso para criterios de capacidad, amortización… La de transacciones para volúmenes, montos, etc. que se mueven en tiempo real. La de amenazas y ataques para determinar áreas más expuestas y optimizar la propia inversión de IT y Seguridad. Las posibilidades al alcance de la mano son infinitas, la imaginación es el límite en muchos casos. Ser creativos dará una gran oportunidad de aportar valor y que Ciberseguridad se convierta en una palanca, incluso en un «socio de negocio» clave y fundamental.

CONCLUYENDO

El Gobierno de Ciberseguridad es una necesidad en cualquier organización con cierta complejidad, especialmente relevante en aquellas con una alta dependencia de la tecnología y un uso masivo de lo digital. Debe, por tanto, formar parte del Gobierno Corporativo para lograr sus objetivos, cubriendo no solo las necesidades actuales si no las futuras.

Puede considerarse parte del Gobierno de la Seguridad de la Información y sus objetivos básicos: alineación estratégica, gestión del riesgo, aportación de valor, administración de recursos y evaluación y medición.

La mayor complejidad reside en la visibilidad en la organización, que debe propiciarse con una aproximación y entendimiento correcto por parte de la alta dirección y escala ejecutivas; la escasez de histórico para determinar probabilidad e impacto en la gestión de los riesgos; la extrema volatilidad y nivel de cambio en el entorno digital; la escasez de profesionales cualificados y la capacidad de medir la aportación real y añadida de valor.

Es por tanto, una función con grandes retos, que ha llegado para quedarse y que sufrirá de un vertiginoso incremento de relevancia en todo tipo de organizaciones.

Requerirá por tanto una gestión inteligente, visionaria, de perfiles afectos al cambio y con amplia visión estratégica y de conjunto al mismo tiempo que con la calificación y habilidades técnicas específicas, sin olvidar las habilidades complementarias tan apreciadas en un mundo cambiante.

NOTAS

[1] http://www.cantabriatic.com/federacion-de-las-cmdb/
[2] http://www.normas-iso.com/iso-20000/
[3] https://seguinfo.wordpress.com/category/iso/page/23/
[4] https://www.fundeu.es/recomendacion/segurizar-securizar-securitizar/
[5] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

[6] https://www.certguidance.com/service-catalogue-management-itil/
[7] https://searchcio.techtarget.com/definition/threat-hunter-cybersecurity-threat-analyst
[8] http://www.normas-iso.com/implantando-iso-27001/
[9] https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad
[10] https://debitoor.es/glosario/definicion-de-benchmarking
[11] https://www.incibe.es/protege-tu-empresa/blog/el-factor-humano-control-politica-seguridad
[12] https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf
[14] http://dle.rae.es/?id=JHRSmFV
[15] https://www.avantiperformance.eu/kpi-kri-la-diferencia/
[16] http://www.iso27000.es/
[17] https://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf
[18] https://www.ovtt.org/empresa-base-tecnologica
[19] https://www.riskinsight-wavestone.com/en/2017/04/cyber-due-diligence-business-valuation/