Ciberseguridad
para Ejecutivos.

Una guía orientada a minimizar los riesgos, comprender las nuevas amenazas de la década y como implementar una estrategia éxitosa en su empresa.

CIBERSEGURIDAD
APLICADA A TU NEGOCIO.

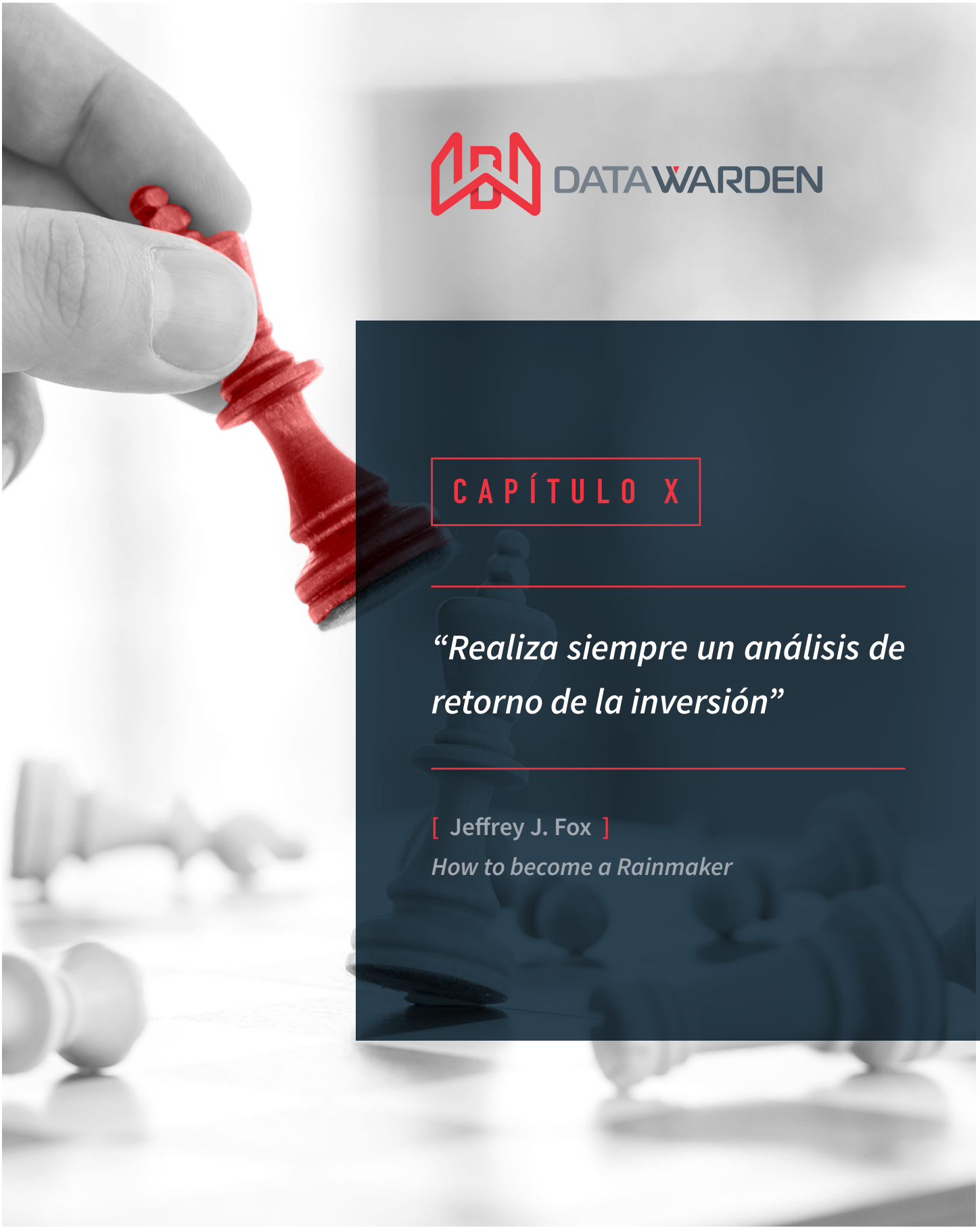
DATAWARDEN

CAPÍTULO X

Retorno de la inversión en seguridad (ROSI)

CIBERSEGURIDAD
APLICADA A TU NEGOCIO.

DATAWARDEN



DATAWARDEN

CAPÍTULO X

“Realiza siempre un análisis de retorno de la inversión”

[Jeffrey J. Fox]

How to become a Rainmaker

Tal y como se ha expresado a lo largo del libro, una de las prioridades del **CIO**, o **CISO, es la gestión efectiva de la seguridad de la información y la aprobación del presupuesto e inversiones necesarios para lograr este objetivo.**

Este proceso **inicia con la evaluación, valoración y priorización de los activos,** y la determinación de los escenarios de amenazas que podrían afectarlos, de manera que se proceda a determinar los riesgos a los que están expuestos y los controles de seguridad que son necesarios, así finalmente se llegaría a dimensionar el costo y justificación financiera para poner en marcha esos controles.

Al monitoreo, la contención de amenazas, la respuesta a incidentes y el cumplimiento regulatorio se le suma la justificación de las inversiones que soportan la estrategia de seguridad, y **todo forma parte de las principales responsabilidades del encargado de la seguridad de la información (CISO) y su equipo de trabajo.**

Las situaciones económicas hostiles, complicadas y recesivas, generadas por cuestiones de orden global, como la pandemia por covid-19, **propician una situación compleja para las organizaciones al momento de adoptar y tomar decisiones de inversión,** sobre todo cuando van más allá de la posible generación de ingresos, elaboración de nuevos productos o reducción del gasto operativo para mantenerse competitivos.

Por otro lado, a esta situación, ya de por sí compleja, se le ha sumado una ola de ataques, robos de información y extorsiones que amenazan la continuidad de las operaciones empresariales y afectan directamente el valor del negocio para los accionistas y su rendimiento. **Esta es una oportunidad importante para conseguir fondos para la estrategia de seguridad,** que debemos saber justificar apropiadamente.

En respuesta a lo anterior

Los líderes de negocio necesitan que el CISO adopte un liderazgo estratégico, que vaya más allá del monitoreo, cumplimiento y operaciones de seguridad, que se integre de mejor forma al negocio, que proponga soluciones innovadoras y efectivas en costo, es decir, que administre el riesgo de una forma estratégica e integrada a las áreas de negocio, y que trabaje en crear una cultura de propiedad del riesgo cibernético compartido con la organización.

Algunos de los aspectos relevantes** que permiten que el CISO, o responsable de la seguridad, **sea exitoso y consiga los fondos necesarios para la estrategia de seguridad:

Es que piense de forma innovadora y austera, que considere que los aspectos de control que defina sean habilitadores de negocio, que alinee eficientemente las acciones de protección y determine con claridad el retorno de la inversión en seguridad (**ROSI** por las siglas en inglés: ***return on security invesment***), a fin de que incremente las posibilidades de ser aprobado.

Como sabemos, **el análisis del retorno de la inversión permite calcular los beneficios económicos que obtendrá el negocio al iniciar alguna estrategia o al utilizar cierta solución.**

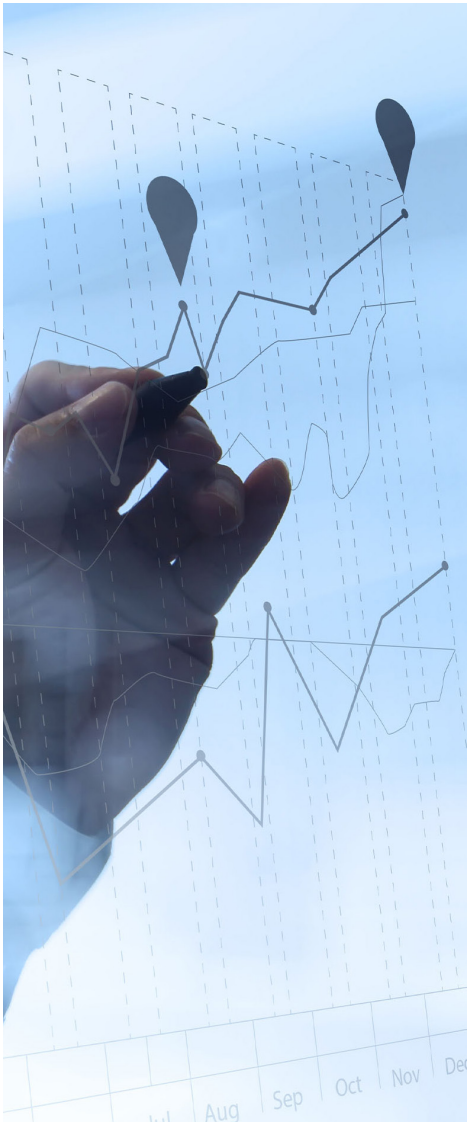
Cuando hablamos de seguridad, las cosas no cambian, sólo es necesario darle un enfoque orientado al riesgo y al valor de los activos que vamos a proteger.

Una definición apropiada para el ROSI señala que se trata del indicador financiero que establece el punto de retorno máximo de la inversión en seguridad, y equivale a la situación en la que el costo total de la habilitación de medidas de seguridad es el más bajo e incluye el costo de los eventos de seguridad, el costo de los controles de seguridad diseñados para prevenirlos o contenerlos en forma apropiada y el costo de los recursos humanos y tecnológicos para operarla y mantenerla.

Para el profesional de la seguridad, el ROSI es significativamente más importante que el ROI, ya que permite explicar en forma efectiva las necesidades de inversión.

Es precisamente en este punto donde los dueños del negocio, los directores de finanzas y los contralores suelen entender la estrategia de protección o de ciberseguridad y facilitan la aprobación de la inversión; no obstante, **es también el momento en que les surgen diversas preguntas que usted debe estar preparado a contestar.**

Principalmente tenemos que mostrar, por ejemplo, que no estamos gastando $100,000 dólares para proteger un activo valorado en $10,000 dólares, ni uno que sólo generará $50,000 dólares en ingresos. Como parte de este proceso, **es importante garantizar que estamos alineados con la estrategia del negocio y con su propuesta de valor,** y que entendemos el entorno de los activos y los riesgos o amenazas a los que están expuestos.



Por lo tanto, es necesario que la alta dirección, finanzas, los dueños de los procesos críticos de negocio y el responsable de la seguridad compartan y entiendan las estrategias y necesidades de protección, y por consiguiente el gasto o inversiones en seguridad de información que se requieren, **y que verifiquen que el retorno de inversión sea acorde con el riesgo identificado.**

Realizar esta estimación nos permite ganar credibilidad y ser considerados parte del negocio, y no sólo un ave de mal agüero que porta noticias de ataques de alto impacto no detectados oportunamente o que notifica que no debe llevarse a cabo un proyecto estratégico del negocio porque no cumple con elementos de seguridad.

El hecho de que la alta dirección normalmente se sienta atraída por las actividades que generan más ingresos o ganancias (pues es su principal motivación) hace importante que planteemos estrategias innovadoras, pero también efectivas y prácticas, **que permitan la reducción de pérdidas o fraudes y/o que sean habilitadoras de nuevos negocios.**

Trabajar a tiempo es importante; debemos tener en mente que la implementación oportuna de controles de seguridad reduce la probabilidad de pérdidas elevadas en caso de que ocurra un **incidente de seguridad.** La cultura reactiva ante incidentes siempre va a ser más costosa, ya que no sólo se orienta a resolver el daño sino a recuperar la imagen y saldar las posibles penalizaciones o pérdidas resultantes del incidente.

Para determinar la mejor estrategia de protección e inversión requerida, **la organización necesita entender y analizar los factores y escenarios asociados, así como los costos de proteger la información.** Es importante incluir factores como el rendimiento o productividad, la disponibilidad y la cobertura de los controles en los que se realizará la inversión como parte del análisis de riesgos y costos.

Recuerde que es necesario contar con una evaluación, o al menos con un registro de riesgos o amenazas a los que están expuestos los activos; es decir, en términos contables es necesario establecer el libro mayor de riesgos, que debe incluir la ocurrencia o expectativas de ocurrencia de dicho riesgo, así como las pérdidas potenciales esperadas en caso de que se materialice.

No importa si este registro se realiza en una hoja de cálculo o una base de datos, **lo importante es que los riesgos que enfrentan los activos críticos sean visibles** y se muestren en un lenguaje claro que entiendan las diferentes áreas de negocio.

Tenga en mente que no debe ir a la alta dirección a vender un producto; por el contrario, debe presentar los beneficios o aspectos de valor que va a obtener la organización con este producto, solución o estrategia; esto hará una diferencia significativa al momento de presentar la propuesta y obtener la aprobación.

Asegúrese de cumplir las expectativas y necesidades de los dueños o responsables de los servicios críticos o estrategias del negocio; trabaje activamente con ellos y entienda sus necesidades y limitaciones, así como el valor de los activos o la capacidad de éstos para generar el negocio.

Una vez determinados estos aspectos, es importante establecer los escenarios de amenazas, riesgos o pérdidas a los que están expuestos los activos críticos a proteger, plantearlos en términos reales a fin de explicar qué tipo de contención de riesgos se está implementando, su alcance y, por supuesto, el impacto estimando o el beneficio y el costo asociado en caso de implementar dichos controles.

Por tanto, es importante que realice una calificación de dichos riesgos e impactos con un enfoque lo más cuantitativo posible y, si eso no es posible, uno semicuantitativo, manteniendo el foco en el tipo de operaciones o funciones de negocio que soportan dichos activos.

Considere que, mediante la visibilidad de los diferentes escenarios de riesgo o amenaza, y la determinación del impacto o amenazas reales, podrá establecer un marco cuantificado de los riesgos, así como el costo de mitigación, lo cual le permitirá entregar una estimación financiera aproximada a la dirección o a sus pares a nivel ejecutivo.

Es clave considerar que los responsables de la toma de decisiones y de la aprobación de las inversiones financieras están acostumbrados a recibir propuestas o requerimientos de inversión en presentaciones modernas, simples, directas y con números reales. Evite en la medida de lo posible llevar el ámbito técnico de seguridad o de **FUD *(fear, uncertanty & doubt),*** es decir, temor, falta de certeza o duda, a quienes toman las decisiones, pues esto generalmente termina mal y no es una práctica apropiada para gestionar seguridad, ya que puede desencadenar en pérdida de relevancia de lo que se está presentando.

A fin de lograr una estimación lo más cuantitativa posible, un enfoque comúnmente utilizado para materializar o dimensionar el ROSI es el siguiente:

En primer lugar, debe estimar el daño potencial que un incidente podría causar a la organización, que también se denomina **SLE *(single lost expectancy)*** y para calcular el SLE debe considerar aspectos como:

- El impacto y alcance del posible incidente, esto es, qué departamentos, ubicaciones, unidades de negocio y procesos se verían afectados.
- **El costo que implicaría la compra o restauración de equipos, bienes y materiales que resultarían dañados por el incidente.**
- La mano de obra requerida, es decir, el costo de los recursos internos o externos que resolverían el incidente.
- **Penalizaciones regulatorias y/o contractuales. Hoy en día las organizaciones a las que ofrecemos servicios o los órganos regulatorios han establecido multas por una falla o afectación del servicio o pérdida de información.**

- **Pérdida de ingresos.** Este es el aspecto que seguramente tendrá más eco en la dirección, sobre todo si se plantea en términos de pérdida de ingresos de clientes actuales, potenciales, pérdida de clientes y afectación a la marca.

A continuación, **debemos estimar la probabilidad de ocurrencia:** aquí es cuando entran los escenarios planteados con anterioridad y se consideran las amenazas, impactos y vulnerabilidades, así como las medidas de seguridad existentes.

Un aspecto crucial es la determinación de la frecuencia estimada en la que se producirá un incidente de este tipo: **puede ser semestral, anual o realmente muy poco probable.**

Es importante ser realista y aprovechar su matriz de riesgos con las aproximaciones o amenazas. En caso de que faltara esta información, existen sitios como el **Ponemon Institute,** que lleva estadísticas de eventos, valoraciones e impactos financieros derivados de los distintos ataques de ciberseguridad. Incluso existen diferentes reportes de fabricantes o proveedores de seguridad que hablan de la experiencia de clientes similares o en diferentes industrias.

Veamos a *estimación del costo* anualizado de riesgo algunas acciones clave para lograr este objetivo.

Single lost expentancy (SLE) probabilidad de ocurrencia estimada = annual lost expectancy (ALE).

Ahora se trata de evaluar los beneficios de los controles, y a lo que nos referimos es a **determinar la frecuencia del incidente potencial y su impacto después de implementar las medidas de seguridad.** Es importante reconocer que, en la mayoría de los casos, no podemos evitar la frecuencia de ocurrencia de un evento de seguridad, pero sí podemos minimizar el impacto de su ocurrencia.

Por último, al estimar el costo total de los controles de seguridad, **es importante tener en cuenta varios aspectos:**

1 Valor de compra

Incluya los diferentes costos, como el hardware, software, servicios de implementación y recursos externos a utilizar.

2 Valor residual del control de seguridad

Considere el valor para la organización después de que ya no esté en uso e incluya la depreciación.

3 Costos de mantenimiento y soporte

Las tecnologías necesitan mantenimiento, reparaciones, reposición y soporte en general para mantenerse vigentes, sobre todo las de seguridad.

4 Costos de operación

Es decir, el personal interno que se dedicará a operar, monitorear y mantener el control, funcionalmente hablando.

El director de finanzas le agradecerá contar con esta información, sobre todo porque con estos elementos podrá determinar si el retorno de la inversión en seguridad es positivo o no. **El punto de equilibrio es cuando la disminución de su riesgo es mayor que el costo total de las medidas de seguridad e implicaciones de mantenerla.**

Al calcular ambos en forma anual podrá validar que su expectativa de pérdida anualizada es mayor que el costo anual de las medidas de seguridad, **y precisamente éste sería el momento en el que el ROSI se vuelve crucial para la toma de decisiones y aprobación de su estrategia.**

Recuerde que, adicionalmente, a la dirección le interesa saber:

¿Cómo está el entorno externo?

¿Qué están haciendo sus pares o competidores?

¿Cómo se comparan con ellos?

Por esta razón, **le recomendamos investigar al respecto antes de ir a presentar su estrategia y requerimientos de aprobación.** Actualmente existen empresas que realizan este tipo de servicios y que suelen ser muy útiles para la dirección, ya que muestran información externa del nivel de riesgos visto desde la perspectiva de un tercero.

Idealmente, **el proceso de definición de requisitos debe comenzar desde la parte superior de la organización.**

Comprender todos los procesos empresariales es importante para garantizar que los cambios en los procesos de gestión o mantenimiento se llevan a cabo correctamente desde la perspectiva de seguridad.

La manera en que una organización se enfoca en la protección de la información depende de su apetito por el riesgo. **La alta dirección necesita considerar el impacto para la organización, si no mitigan adecuadamente los riesgos,** y es importante que el CISO se asegure de que esto sea claro, oportuno y se avale por los dueños de los procesos de negocio, sin tener que estar en modo reactivo.

Esperamos que pronto las organizaciones transformen su cultura organizacional, presten atención y asignen recursos humanos y financieros al programa de seguridad de la información, y no esperen a actuar exclusivamente después de que se haya producido un evento o brecha significativa.

Es mejor que sean proactivos y aseguren la resiliencia del negocio, aun en los diferentes escenarios que nos presenta la nueva realidad de los negocios.

DATAWARDEN

¡Contáctanos!

Nuestros **asesores especializados** están listos para atenderte.

CDMX

Constituyentes 1070, PB-9, Colonia Lomas Altas,
Alcaldía Miguel Hidalgo. C.P. 11950.
CDMX.

Teléfono

(+52) 55 5370 6270

Atención

24/7

ventas@datawarden.com

datawarden.com