Riesgo positivo dentro de la ciberseguridad

AWS Orientación prescriptiva

AWS Orientación prescriptiva: Riesgo positivo dentro de la ciberseguridad

Table of Contents

Riesgo positivo dentro de la ciberseguridad

Greg Bell, Amazon Web Services (AWS)

mayo de 2022 (historial de documentos)

La mayoría de las personas piensa en el riesgo desde una perspectiva negativa, como la exposición a una pérdida o la gestión de un evento adverso. Sin embargo, la definición de riesgo de la Organización Internacional de Normalización (ISO) es el “efecto de la incertidumbre en los objetivos”. En este caso, el efecto puede ser positivo o negativo.

Los riesgos reales pueden variar de un sector a otro, pero esta definición estándar se aplica a todos, y cada sector tiene riesgos tanto negativos como positivos. En el sector de la ciberseguridad, el riesgo negativo se refiere a una pérdida potencial y el riesgo positivo se refiere a la posible ganancia de activos, conocimientos, mejoras o datos.

Los dominios de gestión de proyectos y TI han adoptado la estrategia de evaluar los riesgos positivos en los informes y las decisiones empresariales. Sin embargo, esta todavía no se ha adoptado como una práctica habitual en el sector de la ciberseguridad, y muchas metodologías de gestión de riesgos aún se centran en los riesgos negativos. Si se menciona el riesgo positivo, es solo brevemente.

En la ciberseguridad, siempre se consideró el riesgo exclusivamente desde una perspectiva negativa. Los dos tipos más comunes de riesgo negativo en el campo de la ciberseguridad son los siguientes:

- Riesgo de impacto negativo: exposición a pérdidas causadas por factores externos, como una amenaza. Por ejemplo, los ciberdelincuentes pueden provocar un incidente de seguridad o aumentar la probabilidad de que ocurra.
- Riesgo de impacto positivo: exposición a pérdidas en busca de una ganancia, como una vulnerabilidad producto de un cambio. Por ejemplo, al implementar una estrategia de TI, puede aumentar la posibilidad de que se produzca un incidente de seguridad sin que usted lo advierta. El riesgo de impacto positivo no es lo mismo que riesgo positivo. A pesar de que se produce en busca de una ganancia, el riesgo de impacto positivo se centra en la probabilidad de pérdidas.

Hasta hace poco, la ciberseguridad solo consideraba el riesgo negativo, y la definición de riesgo se centraba en un posible resultado negativo. Los riesgos positivos se centran en el posible resultado positivo al principio de la identificación del riesgo. La exclusión del riesgo positivo hace que no se reconozcan los resultados positivos en materia de ciberseguridad. Debido a que se centran en

el riesgo negativo, los líderes ejecutivos suelen percibir la ciberseguridad como algo reactivo en lugar de proactivo y subestiman la contribución de la ciberseguridad a los resultados empresariales positivos.

En este documento se define el riesgo positivo para el sector de la ciberseguridad y se analizan los beneficios y la importancia de incluir los riesgos positivos en la estrategia de ciberseguridad.

Beneficios del riesgo positivo

Especialmente en un sector como el de la ciberseguridad, que se centra en proteger a la empresa de posibles pérdidas, es más fácil abordar el riesgo desde una perspectiva negativa. Replantear los riesgos de ciberseguridad en función de sus posibles beneficios puede beneficiar a la empresa al promover resultados positivos, aumentar la postura de seguridad de la organización y aumentar la confianza de los clientes.

Promoción de resultados positivos

La adopción de un riesgo positivo permite a la organización evaluar y reconocer la contribución que el dominio hace a los resultados empresariales positivos. Según La ciberseguridad en la alta dirección y en la sala de juntas (Informe de investigación del Grupo de Estrategia Empresarial):

- El 69 % de los líderes empresariales y tecnológicos cree que la ciberseguridad es, en su totalidad o en su mayor parte, un área tecnológica con poca o ninguna vinculación con la empresa.
- El 11 % de los líderes empresariales y tecnológicos equiparan la ciberseguridad con la conformidad normativa.
- El 82 % de las organizaciones afirma que los riesgos de ciberseguridad han aumentado en los últimos dos años debido a factores como el aumento de las ciberamenazas, una mayor integración de la tecnología en la empresa y una superficie expuesta a ataques cada vez mayor.

Cuando los ejecutivos de ciberseguridad integran el riesgo positivo en las conversaciones y los informes, esto permite promover el valor de las operaciones de TI seguras dentro de la empresa.

Por ejemplo, supongamos que una empresa sufrió una filtración de datos hace varios años que se debió a la falta de un proceso de administración de revisiones. Los medios de comunicación siguen mencionando el incidente y esto afecta a las percepciones de los clientes sobre la empresa y sus interacciones con ella. La empresa quiere superar el incidente y ampliar su oferta de servicios, pero la confianza de los clientes bloquea las ventas. La ciberseguridad aprovecha el riesgo positivo para convencer a los líderes de que inviertan en un proceso de administración de revisiones que actualice continuamente las aplicaciones. El nuevo proceso reduce ampliamente el riesgo de una filtración de datos, lo que mejora la postura de seguridad de la empresa. Las noticias del proceso de gestión de up-to-the-minute parches llegan a los medios de comunicación y a los clientes potenciales. Los clientes ahora se sienten cómodos comprando en la empresa y las ventas aumentan a un nivel impresionante.

Si no se tienen en cuenta los riesgos positivos durante la identificación del riesgo, la evaluación puede quedar incompleta y afectar la decisión empresarial. Para ver ejemplos concretos de riesgos positivos que podrían afectar las decisiones empresariales, consulte Ejemplos de riesgo positivo.

Aumento de la postura de seguridad y la confianza de los clientes

La ciberseguridad es parte integral de la postura de seguridad de la empresa. Las filtraciones de datos pueden afectar la confianza de los clientes de forma negativa, pero una postura de seguridad y una reputación sólidas también pueden aumentar la confianza de los clientes e impulsar las oportunidades de negocio.

Como se explica en Promoción de resultados positivos, mediante las investigaciones se demostró que el liderazgo ejecutivo comprende los riesgos negativos asociados a la ciberseguridad, pero con frecuencia no comprende el riesgo positivo o el valor empresarial. Sin embargo, también se demostró que los líderes en ciberseguridad entienden cómo una postura de seguridad sólida puede beneficiar a la organización.

En Investigación sobre ciberseguridad: el acelerador de la innovación (documento técnico de Vodafone), Vodafone entrevistó a 1434 responsables de la toma de decisiones en ciberseguridad de todo el mundo. Según sus datos:

- El 73 % de los encuestados cree que una seguridad sólida crea nuevas oportunidades de negocio.
- El 89 % afirmó que las mejoras en su seguridad aumentarían la fidelidad y la confianza de los clientes.
- El 90 % también ha declarado que ha conseguido mejorar su imagen, llegar a nuevos clientes potenciales y convertirlos en clientes reales.
- El 89 % cree que tener una ciberseguridad eficaz es una ventaja competitiva importante, que les ayuda a diferenciarse de sus competidores.
- El 24 % informó de un aumento en sus ingresos gracias al uso de tecnologías en la nube y el Internet de las cosas (IOT) y a la adopción de controles de seguridad de TI específicos.
- En lugar de utilizar los posibles resultados negativos al comunicarse con los líderes ejecutivos, también puede utilizar el riesgo positivo para comunicar el valor empresarial de mejorar la confianza de los clientes. Los ejecutivos pueden ser cautelosos a la hora de financiar programas. En algunos casos, la ciberseguridad requiere lo mínimo necesario para funcionar. La comunicación interna de los riesgos positivos en las solicitudes de financiamiento puede ayudar a sus líderes a comprender el valor empresarial de la ciberseguridad. Esto puede traducirse en un aumento del financiamiento para las iniciativas de ciberseguridad y generar ingresos para la empresa.

Cambio en el lenguaje de riesgos de ciberseguridad

Parte del desafío de adoptar el riesgo positivo para la ciberseguridad es que la terminología técnica y específica del dominio se centra en el riesgo negativo, como las amenazas, las vulnerabilidades y los controles de seguridad. El sector de la ciberseguridad debe evolucionar y ampliar su vocabulario para incluir un lenguaje que haga hincapié en los resultados empresariales positivos (o los riesgos positivos) que la ciberseguridad aporta a la empresa. Con términos como ventaja de negocio, beneficios y valor de negocio, se destaca la contribución de la ciberseguridad a la organización.

Cambiar el lenguaje de la ciberseguridad permite cambiar la percepción de que la ciberseguridad es un área tecnológica que se centra exclusivamente en las amenazas y las vulnerabilidades y que está desvinculada de la empresa. Los líderes empresariales suelen subestimar la contribución de la ciberseguridad a los resultados empresariales positivos. Para obtener más información sobre la percepción de la ciberseguridad por parte de los líderes, consulte Promoción de resultados positivos.

Aumento de la adopción en campos relacionados

Hay cada vez más interés en muchos campos por incluir el riesgo positivo, ya que este reconoce las contribuciones del dominio a los resultados empresariales. El concepto de riesgo positivo se ha incorporado recientemente a los procesos y definiciones comunes de la gestión de proyectos.

En 2013, el Instituto de Gestión de Proyectos (PMI) incorporó la definición de riesgo positivo (también denominado oportunidades) en la quinta edición del Conjunto de Conocimientos sobre Gestión de Proyectos (PMBOK). En el PMBOK, se define el riesgo individual como “un evento o una condición inciertos que, si ocurren, tienen un efecto positivo o negativo en uno o más objetivos del proyecto”. Se define en términos generales el riesgo del proyecto como “el efecto de la incertidumbre en el proyecto en su conjunto... es más que la suma de los riesgos individuales de un proyecto, ya que incluye todas las fuentes de incertidumbre del proyecto... y representa la exposición de las partes interesadas a las implicaciones de las variaciones en los resultados del proyecto, tanto positivas como negativas”.

Lamentablemente, la inclusión de los resultados positivos por parte del PMI en sus definiciones de riesgo aún no se aplica al sector de la ciberseguridad.

Ejemplos de riesgo positivo

Los siguientes son algunos ejemplos del riesgo positivo en la tecnología, la gestión de proyectos y la ciberseguridad.

Riesgo positivo en la tecnología

Un ejemplo de riesgo positivo en la tecnología es que la implementación de una tecnología podría conducir a una reducción del costo de los salarios. Por ejemplo:

1. La implementación de la tecnología podría conducir a una mayor eficiencia empresarial.
2. Estas eficiencias podrían lograr una reducción de la mano de obra.
3. La reducción de la mano de obra podría minimizar el costo de los salarios.

Riesgo positivo en la gestión de proyectos

Un ejemplo de riesgo positivo en la gestión de proyectos es que un error de cálculo en el presupuesto de un proyecto podría suponer un ahorro de costos o el financiamiento de proyectos adicionales. Por ejemplo:

1. La implementación temprana de un proyecto tecnológico podría provocar que el director del proyecto calcule mal los costos del proyecto.
2. Calcular mal los costos del proyecto podría generar fondos excesivos para el proyecto.
3. Un exceso de fondos para proyectos podría suponer un ahorro de costos o el financiamiento de proyectos adicionales.

Riesgo positivo en materia de ciberseguridad

Un ejemplo de riesgo positivo en materia de ciberseguridad es que la implementación de la gestión de revisiones podría aumentar la confianza de los clientes. Por ejemplo:

1. La implementación de la administración de revisiones podría reducir las vulnerabilidades en la aplicación.
2. Eliminar las vulnerabilidades podría minimizar los riesgos de las aplicaciones y hacerlas más seguras.

3. La mejora de la seguridad de las aplicaciones podría limitar la pérdida de datos.
4. La reducción de la pérdida de datos podría aumentar la confianza de los clientes.

Otro ejemplo de riesgo positivo en materia de ciberseguridad es que la implementación de la respuesta a incidentes podría aumentar la productividad de los empleados. Por ejemplo:

1. La implementación de la respuesta a incidentes podría conducir a la detección de un aumento del tráfico de red.
2. El aumento del tráfico de la red podría permitir la detección del uso indebido de los recursos por parte de los empleados que accedan a contenido que no esté relacionado con el trabajo, como los servicios de streaming de música y video. Estas actividades consumen ancho de banda de la red y pueden afectar negativamente el rendimiento de la red y las aplicaciones.
3. La detección del uso indebido de los recursos de la empresa por parte de los empleados podría provocar el bloqueo de estos servicios.
4. El bloqueo de estos servicios podría reducir el consumo de ancho de banda de la red y aumentar la productividad de los empleados.

Por último, el último ejemplo de riesgo positivo en materia de ciberseguridad es que la implementación de un plan de respuesta a incidentes podría aumentar las oportunidades comerciales y la conformidad con las leyes de privacidad. Por ejemplo:

1. La implementación de un plan de respuesta a incidentes podría permitir detectar e identificar rápidamente malware y ransomware.
2. La identificación de malware y ransomware podría minimizar el impacto y mitigar la amenaza a los recursos de la empresa.
3. Mitigar la amenaza a los recursos de la empresa podría generar nuevas oportunidades comerciales y ayudar a la empresa a cumplir con las leyes de privacidad.

Respuesta a los riesgos de ciberseguridad

Las respuestas a los riesgos positivos y negativos son muy diferentes. En el caso de los riesgos negativos, se toman medidas para minimizar el impacto en el resultado; sin embargo, en el caso de los riesgos positivos, se toman medidas para maximizar el impacto en el resultado. En la siguiente tabla, se muestran las posibles respuestas a los riesgos positivos y negativos.

Tipo de riesgo	Respuesta	Definición
Riesgo positivo	Explotar	Maximice la probabilidad de que se produzca el riesgo para obtener su efecto positivo.
	Share	Asigne parte de la propiedad o de la responsabilidad del riesgo a otra parte. Se trata del mismo enfoque que se adopta con un riesgo negativo y se intenta controlar las posibles pérdidas o ganancias .
	Mejorar	Aumente las condiciones que crean el riesgo para maximizar la oportunidad.
	Ignore	Ignore la posibilidad del riesgo y no tome ninguna medida. Esta respuesta es común cuando la probabili dad del riesgo es muy baja o cuando los beneficios de un posible resultado positivo son mínimos.

Tipo de riesgo	Respuesta	Definición
Riesgo negativo	Mitigar	Minimice la probabilidad de que se produzca el riesgo.
	Transferir	Transfiera la responsabilidad por el riesgo a otra parte, por ejemplo, mediante la adquisición de una póliza de seguro para transferir el riesgo a una compañía de seguros.
	Evitar	Elimine las condiciones que crean el riesgo.
	Aceptar	Reconozca la existencia del riesgo, pero no tome ninguna medida.

En el caso de los riesgos negativos, en las organizaciones se evita, transfiere, mitiga o acepta el riesgo en función de su tolerancia al riesgo y el tipo de riesgo. Se intenta evitar que ocurra y, si ocurre, se intenta minimizar su impacto en la misión general.

La mejor manera de ilustrar las respuestas positivas al riesgo es mediante ejemplos:

- Explotar: un ejecutivo de seguridad se entera de que un profesional de seguridad bien cualificado ha decidido recientemente buscar un nuevo empleo y recibe una generosa bonificación por contratación para atraer al posible empleado a su equipo.
- Compartir: un líder de una unidad de negocios desea mejorar la seguridad mediante un producto de administración de acceso con privilegios, pero no cuenta con presupuesto suficiente para adquirir las herramientas y los servicios en el año fiscal en curso. El líder trabaja con un líder de otra unidad de negocios, quien comprará e implementará la herramienta como un proyecto piloto y, más adelante, ampliará la instalación para dar soporte a ambas unidades de negocios.
- Mejorar: un empleado ha identificado la oportunidad de automatizar un proceso empresarial existente para reducir las amenazas a la ciberseguridad, pero requiere una inversión de tiempo y equipo. Al ver los beneficios de este proceso, el gerente aprueba las horas extra de trabajo para

desarrollar la capacidad y reutiliza los recursos de equipo y software existentes para permitir que el proyecto continúe.

- Ignorar: un ejecutivo de finanzas se entera de que un empleado del departamento de ventas ha desarrollado una nueva aplicación que automatiza una tarea tediosa y manual. Recientemente, se autorizó el uso de la aplicación únicamente en el departamento de ventas. El ejecutivo de finanzas obtiene una copia de la nueva aplicación para conseguir una ventaja similar en su departamento, sin autorización explícita.

Pasos a seguir a continuación

Los dominios de la tecnología y la gestión de proyectos han incorporado los riesgos positivos en sus procesos de evaluación de riesgos, pero el sector de la ciberseguridad los ha excluido históricamente. Los riesgos positivos pueden traducirse en resultados empresariales positivos, y el sector de la ciberseguridad debe hacer la transición para aceptar los riesgos positivos y obtener los beneficios.

Puede empezar a informar los riesgos positivos de forma inmediata en todas las comunicaciones. Por ejemplo, las evaluaciones de riesgos, las evaluaciones de seguridad o los informes de estado deben incluir una sección sobre los riesgos positivos. Las solicitudes de financiamiento dirigidas a la dirección ejecutiva deben incluir los riesgos positivos, comunicar los posibles beneficios para la empresa y destacar las posibles ventajas empresariales que se obtengan al aprobar la solicitud.

Preguntas frecuentes

¿Cuál es la diferencia entre el riesgo de impacto positivo y el riesgo positivo?

A pesar de que el riesgo de impacto positivo y el riesgo positivo suenan similares, en realidad son muy diferentes. Dentro del riesgo, hay un resultado positivo o negativo, y dentro de los resultados negativos, hay una oportunidad o una amenaza.

Riesgo positivo es la ganancia potencial de activos, conocimientos, mejoras o datos. Por ejemplo, se implementa la administración de revisiones y un proceso para eliminar las vulnerabilidades rápidamente, como en el plazo de una semana. Durante el próximo año, no tendrá ningún incidente de seguridad.

Riesgo de impacto positivo es la exposición a pérdidas en busca de una ganancia. Por ejemplo, en la empresa se instala una nueva aplicación y se implementa la administración de revisiones y un proceso para eliminar las vulnerabilidades rápidamente, como en el plazo de una semana. La exposición a pérdidas (el periodo en el que se eliminan las vulnerabilidades) busca obtener beneficios (una aplicación más segura), por lo que se considera un riesgo de impacto positivo. Puede aumentar el riesgo de impacto positivo cambiando el proceso para eliminar las vulnerabilidades a un día, o reducirlo si cambia el periodo a un mes. Básicamente, el riesgo de impacto positivo es la posibilidad incierta de obtener beneficios mientras se intenta minimizar una pérdida.

¿Por qué es importante incluir el riesgo positivo en la ciberseguridad?

La integración de los riesgos positivos en las evaluaciones y conversaciones sobre los riesgos de ciberseguridad ayuda a promover el valor de la ciberseguridad para la empresa. Para obtener más información, consulte Beneficios del riesgo positivo.

Recursos

- La ciberseguridad en la alta dirección y en la junta (Informe de investigación del Grupo de Estrategia Empresarial)
- Investigación sobre ciberseguridad: el acelerador de la innovación (Documento técnico de Vodafone)
- Integración de la ciberseguridad y la gestión de riesgos empresariales (ERM) (publicación del NIST)
- Definición del riesgo “de impacto positivo” y “positivo” (entrada en el blog del instituto FAIR)

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial	—	27 de mayo de 2022

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.