INFLUENCIA DE LA AGNOTOLOGÍA EN LA GESTIÓN DE LA SEGURIDAD EMPRESARIAL "SHADOW SECURITY" MECANISMO PARA LA GENERACIÓN DE IGNORANCIA

COMPARTE: CARLOS ALFONSO BOSHELL NORMAN (CCO®)-(PPE®)

Esta semana, en clase de formación de los futuros Oficiales de Cumplimiento Integrales, mientras analizábamos las principales causas de las conductas corruptas e ilegales de las personas, pero especialmente en las organizaciones, a pesar de todas las políticas y los sistemas de prevención de adopción obligatoria y voluntaria, Alejandro, un alumno, nos recordó acertadamente lo que es la AGNOTOLOGÍA, y sus implicaciones directas en las actuaciones de las personas. Revisémonoslo con mayor detalle:

La agnotología es el estudio de la producción cultural de la ignorancia, la duda o la desinformación deliberada que tiene un impacto profundo y a menudo subestimado en la gestión de la seguridad empresarial, en particular de cómo se produce y se mantiene la ignorancia o la duda en temas específicos, muchas veces de manera intencionada. Esta disciplina analiza, por ejemplo, cómo ciertos grupos o intereses pueden generar desinformación o confusión para afectar la percepción pública o decisiones.

En el entorno corporativo actual, la ignorancia ya no es simplemente una falta de conocimiento; con frecuencia es una estrategia diseñada por actores hostiles o un subproducto de la saturación informativa. Para un director de seguridad, entender cómo se fabrica la duda es crucial para proteger los activos, la reputación y la continuidad del negocio.

- **Concepto de agnotología y su relevancia en el contexto organizacional**

La agnotología es el estudio de la producción y gestión deliberada de la ignorancia o el desconocimiento, especialmente en contextos donde la información es manipulada o suprimida con fines específicos. En el ámbito empresarial, la agnotología adquiere relevancia al analizar cómo la falta de conocimiento ya sea intencionada o accidental, puede influir en la gestión de la seguridad. La seguridad organizacional depende en gran medida del conocimiento profundo de la industria, la tecnología utilizada y las mejores prácticas en seguridad. La ausencia o distorsión de este conocimiento puede generar vulnerabilidades significativas, ya que impide la identificación y mitigación efectiva de riesgos. Por tanto, la agnotología

proporciona un marco conceptual para entender cómo la ignorancia, ya sea inducida por desinformación o por omisión, puede afectar la toma de decisiones y la implementación de políticas de seguridad dentro de las empresas.

- **Fundamentos para la gestión del conocimiento y la ignorancia en la seguridad empresarial**

La gestión de la seguridad empresarial requiere una evaluación minuciosa de la organización, identificando debilidades y precauciones críticas. Este proceso implica no solo la adquisición de conocimiento, sino también la identificación de áreas donde la ignorancia puede ser perjudicial. La agnotología fundamenta la importancia de diagramar la organización en equipos funcionales, de soporte y estructura corporativa para comprender plenamente las vulnerabilidades de seguridad.
El análisis de la postura de seguridad y la identificación de debilidades abarcan tanto la estructura física como la red informática, el software y el personal de la empresa. La ignorancia en cualquiera de estos ámbitos puede ser explotada por amenazas internas o externas, lo que subraya la necesidad de políticas de seguridad robustas y programas de formación continua para el personal.
Así, la agnotología no solo alerta sobre los peligros de la ignorancia, sino que también orienta la creación de estrategias para contrarrestarla mediante la generación, difusión y aplicación efectiva del conocimiento en todos los niveles de la organización.

- **Factores sociocognitivos y percepción de la carga de cumplimiento**

En los entornos empresariales, la generación de ignorancia respecto a la seguridad puede estar profundamente influenciada por factores sociocognitivos que afectan la actitud y el comportamiento de los empleados. Diversas teorías interdisciplinarias, como la teoría de la elección racional y la teoría de la motivación de protección (PMT), explican cómo los empleados evalúan los beneficios y costos asociados al cumplimiento de las políticas de seguridad. La percepción de la carga de cumplimiento, es decir, la idea de que seguir las políticas de seguridad puede ser oneroso o perjudicial para la productividad, puede llevar a que los empleados ignoren o minimicen la importancia de ciertas medidas de seguridad. Este fenómeno se ve reforzado cuando los empleados priorizan sus necesidades individuales sobre el cumplimiento altruista de las normas organizacionales, lo que puede derivar en una falta de conciencia o incluso en una ignorancia deliberada sobre los riesgos y consecuencias de la no conformidad.

La evaluación de amenazas y la respuesta a ellas, según la PMT, involucra procesos cognitivos complejos donde los empleados sopesan la gravedad y la vulnerabilidad ante una amenaza, así como la eficacia y el costo de las respuestas protectoras. Si los empleados perciben que los costos de cumplir con las políticas de seguridad superan los beneficios, o si dudan de su capacidad para implementar comportamientos protectores (baja autoeficacia), es probable que opten por ignorar

o subestimar los riesgos, contribuyendo así a la generación de ignorancia organizacional en materia de seguridad.

- **Prácticas de “shadow security” y su invisibilidad organizacional**

Un mecanismo particularmente relevante en la generación de ignorancia es la aparición de prácticas denominadas “shadow security”, (Seguridad en la Sombra). Estas surgen cuando empleados, conscientes de los riesgos de seguridad, consideran que no pueden cumplir con las políticas oficiales y, en consecuencia, desarrollan soluciones alternativas que consideran más adecuadas para su contexto laboral. Estas prácticas, al no estar alineadas con las políticas formales y permanecer ocultas para los responsables de seguridad y la alta dirección, generan zonas de ignorancia institucionalizada. La existencia de “shadow security” refleja un conflicto entre la necesidad de cumplir con los objetivos laborales y la gestión de riesgos, lo que puede llevar a la creación de espacios donde la organización desconoce tanto la naturaleza como la magnitud de los riesgos reales a los que está expuesta.

La invisibilidad de estas prácticas alternativas dificulta la identificación y gestión efectiva de los riesgos, ya que los mecanismos formales de supervisión y sanción no alcanzan a detectar ni corregir estos comportamientos. Así, la organización puede operar bajo una falsa sensación de seguridad, ignorando la existencia de vulnerabilidades críticas que emergen precisamente de la desconexión entre las políticas prescritas y las prácticas reales de los empleados.

- **Impacto de la agnotología en la percepción y gestión del riesgo**

La agnotología, entendida como el estudio de la producción y gestión de la ignorancia, puede influir de manera significativa en la toma de decisiones dentro del ámbito de la seguridad empresarial. En el contexto de la seguridad corporativa, la presencia de información incompleta, ambigua o deliberadamente distorsionada puede afectar la percepción del riesgo y, en consecuencia, las estrategias adoptadas por las organizaciones para proteger sus activos. La gestión de la ignorancia ya sea intencionada o no, puede llevar a subestimar amenazas emergentes o a priorizar recursos de manera ineficiente, lo que incrementa la vulnerabilidad ante incidentes de seguridad. La agnotología, por tanto, se convierte en un factor crítico que puede condicionar la efectividad de las políticas y procedimientos de seguridad empresarial, especialmente en entornos donde la información sobre amenazas es dinámica y a menudo incierta.

- **Vectores de Influencia de la Agnotología en la Empresa**

La inducción deliberada de ignorancia o confusión afecta a la seguridad en tres frentes principales como son los Ataques de Desinformación y Reputación (Guerra de Información), que mediante la fabricación de dudas los competidores desleales, grupos de interés o actores estatales pueden difundir narrativas falsas o sesgadas

sobre los productos, la solidez financiera o la ética de la empresa. El fin no siempre es hacer que el público crea una mentira, sino destruir la confianza y generar suficiente confusión para que los clientes, inversores o reguladores duden de la organización.

Otro frente lo tenemos en la Ingeniería Social y Ciberseguridad, donde la explotación de la "ceguera cognitiva", permite a los ciberdelincuentes utilizar técnicas agnotológicas al crear contextos falsos pero creíbles (Phishing, Spear Phishing, Deepfakes). La manipulación del riesgo, al saturar a los empleados con alertas contradictorias o procedimientos excesivamente complejos, se genera una "fatiga de seguridad", un estado de ignorancia funcional donde el usuario prefiere obviar los protocolos.

El frente de la complacencia Interna y Sesgos de Dirección ante una Ignorancia deliberada corporativa, a veces, la propia estructura empresarial fomenta la agnotología. Ocurre cuando la alta gerencia prefiere "no saber" sobre ciertas vulnerabilidades o fallos de cumplimiento (compliance) para evitar responsabilidades legales o costos inmediatos. Por ejemplo, el efecto cámara de eco, donde los comités de crisis pueden caer en el sesgo de confirmación, ignorando activamente las señales débiles de riesgo porque contradicen la narrativa oficial de éxito de la compañía.

- **El Impacto en la Matriz de Riesgos y la Toma de Decisiones**

La agnotología distorsiona directamente la **percepción del riesgo**. En la gestión de seguridad tradicional, los riesgos se evalúan en función de la probabilidad e impacto basados en datos históricos y análisis de entorno. Sin embargo, la agnotología altera este modelo introduciendo r**iesgos Invisibilizados, con a**menazas reales que se minimizan deliberadamente mediante contra narrativas (por ejemplo, minimizar el impacto de un cambio regulatorio o una tensión geopolítica en la cadena de suministro). Los f**alsos positivos de amenaza, donde las d**istracciones creadas para que el equipo de seguridad concentre sus recursos y atención en un punto ciego, mientras el ataque real ocurre en otra área.

- **Limitaciones de los mecanismos de disuasión y sanción**

La teoría de la disuasión sostiene que la certeza, severidad y rapidez de las sanciones pueden influir en la decisión de los empleados de cumplir o no con las políticas de seguridad. Sin embargo, la efectividad de estos mecanismos ha sido cuestionada, ya que la mera declaración de penalizaciones no garantiza necesariamente un comportamiento seguro. Cuando los empleados perciben que las sanciones son poco probables, poco severas o difíciles de aplicar, pueden optar por ignorar las políticas, contribuyendo así a la generación de ignorancia organizacional. Además, la conceptualización del cumplimiento como una decisión binaria (“cumplir o no cumplir”) ha sido desafiada por la evidencia de respuestas intermedias, como la adopción de prácticas de “shadow security”, que escapan al control y conocimiento de la organización.

Estas limitaciones evidencian que los mecanismos formales de control pueden ser insuficientes para prevenir la generación de ignorancia, especialmente cuando no abordan las motivaciones subyacentes y las percepciones de los empleados respecto a la utilidad, viabilidad y relevancia de las políticas de seguridad. Por tanto, la gestión de la ignorancia en entornos empresariales requiere una comprensión más profunda de los factores psicológicos, sociales y organizacionales que influyen en el comportamiento de los empleados.

Para concluir, el análisis de la agnotología en el contexto de la seguridad empresarial revela la importancia crítica de comprender y gestionar la ignorancia, tanto intencionada como no intencionada, dentro de las organizaciones. La agnotología, al centrarse en los mecanismos de producción y mantenimiento de la ignorancia, permite identificar factores sociocognitivos, prácticas invisibles como la “shadow security” y limitaciones en los sistemas de disuasión y sanción que afectan la percepción y gestión del riesgo.

La presencia de sesgos gerenciales y la subestimación de riesgos improbables, así como la influencia de heurísticas de supervivencia, demuestran cómo la desinformación y la ignorancia pueden comprometer la toma de decisiones y la resiliencia organizacional ante eventos catastróficos.

Las estrategias empresariales orientadas a mitigar los efectos de la agnotología, como la implementación de tecnologías predictivas y adaptativas, resultan fundamentales para proteger activos, reputación y la confianza del cliente. Asimismo, la revisión de casos y ejemplos evidencia que la gestión sistemática de la ignorancia puede prevenir errores recurrentes y fortalecer la seguridad empresarial. Finalmente, las implicaciones éticas y legales subrayan la necesidad de una gestión responsable de la ignorancia, promoviendo la transparencia y el cumplimiento normativo como pilares para una cultura organizacional resiliente y ética. En suma, abordar la agnotología desde una perspectiva integral es esencial para anticipar, gestionar y mitigar los riesgos emergentes en el entorno empresarial contemporáneo.

Feliz día

CARLOS ALFONSO BOSHELL NORMAN
CRIMINALISTA E INVESTIGADOR CRIMINAL
(CCO®) Certified Compliance Officer.
(PPE®) Professional Polygraph Examiner
CEL. +57 318 883 23 76
Correo: gerencia@cbconsultoresprofesionales.com
www.cbconsultoresprofesionales.com