ESCUELA DE INGENIERÍAS INDUSTRIALES

Departamento: Economía y Administración de Empresas

Área de Conocimiento: Organización de Empresas

TRABAJO FIN DE GRADO

Desarrollo de un protocolo Insider Threat en empresas de base tecnológica. Un enfoque desde la inteligencia y la seguridad.

Grado en Ingeniería de Organización Industrial

Autor: Francisco Javier Sánchez Peña

Tutor: Silvia Regina Arroyo Varela

MÁLAGA, mayo de 2025

AGRADECIMIENTOS:

“A mis padres, por estar siempre ahí, por su ejemplo constante de esfuerzo y sus valores, que han guiado mi camino hasta aquí y, en especial, a Maribel, por acompañarme en la montaña rusa que caracteriza esta etapa, por animarme cuando faltaban las fuerzas y por hacerme sentir que todo es posible.

DESARROLLO DE UN PROTOCOLO INSIDER THREAT EN EMPRESAS DE BASE TECNOLÓGICA. UN ENFOQUE DESDE LA INTELIGENCIA Y LA SEGURIDAD.

Resumen del proyecto:

En un contexto de digitalización acelerada y creciente dependencia del trabajo remoto, las amenazas internas se han convertido en uno de los mayores desafíos para la seguridad organizacional. Este Trabajo Fin de Grado aborda el diseño de un protocolo integral de prevención y mitigación del *insider threat* en empresas de base tecnológica, integrando marcos de inteligencia corporativa, ciberseguridad y análisis conductual.

El estudio incluye una revisión del marco teórico y normativo, una clasificación de los perfiles de insider, y un análisis de factores personales y organizativos que influyen en la deslealtad. A partir de este análisis, se propone un protocolo estructurado bajo el ciclo IPDRR (Identify, Protect, Detect, Respond, Recover) e implementado de forma teórica en la empresa ficticia Cynerdata Solutions, S.L., dedicada al desarrollo de soluciones de ciberseguridad e inteligencia artificial.

El protocolo incorpora herramientas como la analítica de comportamiento (UEBA), medidas organizativas (offboarding estructurado, cultura de seguridad) y evaluaciones sistemáticas (ITVA, ITPE). El trabajo concluye con una reflexión sobre los límites del modelo, proponiendo líneas de mejora y su adaptación a distintos sectores.

Este proyecto busca contribuir a la creación de entornos laborales más seguros, resilientes y conscientes del riesgo que puede suponer el factor humano.

Palabras clave: insider, insider threat, amenaza interna, protocolo, IPDRR, cultura de seguridad, inteligencia, prevención, empresa tecnológica

ÍNDICE

1. INTRODUCCIÓN

"Las personas a menudo representan el eslabón más débil en la cadena de seguridad y son crónicamente responsables del fallo de los sistemas de seguridad." (Schneier, 2000)

"El factor humano es verdaderamente el eslabón más débil de la seguridad." (Mitnick, 2003)

En un mundo donde las tecnologías emergentes avanzan a velocidades vertiginosas y donde los entornos laborales híbridos y remotos se han consolidado como norma, las amenazas a la seguridad de la información ya no provienen exclusivamente del exterior. Cada vez más, los ataques más costosos, silenciosos y devastadores tienen su origen dentro de las propias organizaciones. No se trata de ciberdelincuentes en países lejanos, sino de empleados descontentos, contratistas descuidados o usuarios con acceso legítimo que actúan en contra de los intereses de la entidad. Esta figura, conocida como el *insider*, se ha convertido en uno de los principales vectores de riesgo para las empresas del siglo XXI.

Este Trabajo Fin de Grado nace de una preocupación real y contemporánea: ¿están las empresas tecnológicas preparadas para prevenir y detectar la amenaza que suponen sus propios empleados? Frente a la sofisticación de herramientas como la analítica de comportamiento (UEBA), los sistemas de detección automática o los marcos normativos como el NCSC, existe una necesidad aún más profunda: construir una cultura de seguridad que comprenda al empleado no solo como un recurso, sino como un factor de riesgo y, a la vez, como la primera línea de defensa.

El enfoque propuesto aquí no se limita a un tratamiento técnico del problema, sino que parte de una visión que integra seguridad, inteligencia, análisis conductual, resiliencia organizacional y ética corporativa. Para ello, se ha diseñado un protocolo integral de prevención del insider threat, estructurado bajo los principios del modelo IPDRR (Identify, Protect, Detect, Respond, Recover) y validado conceptualmente en un caso práctico aplicado a una empresa ficticia de base tecnológica: Cynerdata Solutions, S.L.

A través de este trabajo, se busca demostrar que la gestión del riesgo interno no es solo un asunto de firewalls o contraseñas, sino una cuestión estratégica que debe implicar a toda la organización, desde el comité directivo hasta el último empleado.

1.1. JUSTIFICACIÓN

El presente estudio se justifica en un contexto donde la transformación digital ha multiplicado las superficies de ataque y ha difuminado los perímetros tradicionales de seguridad. Con la consolidación del trabajo remoto, el acceso a información crítica se ha descentralizado, los sistemas de protección perimetral se han visto superados, y el comportamiento del usuario se ha convertido en una fuente clave de vulnerabilidad.

Diversos estudios respaldan esta preocupación: según el CISA (2024), el 90 % de los profesionales en ciberseguridad consideran que sus organizaciones son vulnerables a amenazas internas, y el coste medio de un incidente provocado por un insider supera los 16,2 millones de dólares. A ello se suma que la mayoría de estos ataques no son detectados hasta semanas o meses después de haber ocurrido.

Pese a esta evidencia, muchas empresas continúan sin integrar de forma adecuada políticas de mitigación de riesgos internos. En particular, las PYMEs y las startups tecnológicas que, aunque ágiles e innovadoras, suelen carecer de políticas robustas de inteligencia o análisis conductual. Esta brecha representa una gran oportunidad (y urgencia) para proponer soluciones concretas, escalables y multidisciplinarias.

En el marco de los estudios del Grado en Ingeniería en Organización Industrial, resulta especialmente apropiado abordar esta temática desde una óptica que integre tecnología, gestión del talento, procesos organizativos y cultura preventiva. El presente TFG se convierte así en un ejercicio práctico que aúna conceptos de seguridad, inteligencia organizacional y prevención de riesgos laborales, con un enfoque disruptivo y actual.

1.2. OBJETIVOS

Objetivo general:

Diseñar un protocolo integral de prevención y mitigación de amenazas internas (*insider threat*) adaptado a empresas de base tecnológica, integrando marcos de ciberseguridad, análisis de comportamiento, buenas prácticas organizativas y principios de inteligencia corporativa.

Objetivos específicos:

1. Analizar el marco teórico de la seguridad empresarial con foco en la figura del insider y sus tipologías.
2. Investigar los factores psicológicos y organizacionales que influyen en el comportamiento desleal del empleado.
3. Estudiar los principales marcos normativos y metodológicos existentes (SIFMA, NCSC, etc.) aplicables a la gestión del insider threat.
4. Diseñar un protocolo de actuación basado en el ciclo IPDRR y adaptado a una empresa tecnológica ficticia con entorno de trabajo híbrido.
5. Evaluar la eficacia teórica del protocolo mediante indicadores de madurez organizacional, analítica de comportamiento y cultura de seguridad.
6. Proponer medidas de mejora continua, formación y concienciación para la creación de una cultura organizacional orientada a la prevención.

2. METODOLOGÍA

Este Trabajo de Fin de Grado adopta un enfoque cualitativo y documental, centrado en un análisis de fuentes científicas, normativas y manuales técnicos especializados en materia de seguridad de la información e Insider Threat.

El objetivo se centrará en diseñar un protocolo Insider Threat dentro del marco de un departamento de Inteligencia y Seguridad para una empresa ficticia de base tecnológica, aplicando buenas prácticas internacionales y fundamentos teóricos respaldados por la literatura académica.

En cuanto a la recolección y el análisis de la información, se hará basándose en una revisión documental exhaustiva, incluyendo:

- Artículos científicos revisados por pares
- Libros especializados en seguridad, psicología organizacional y criminología
- Manuales técnicos e informes de empresas de ciberseguridad
- TFGs y Tesis doctorales nacionales e internacionales consultadas en bases como Dialnet o Proquest.

Todos estos documentos llevarán consigo unos criterios de selección aplicados a razón de: relevancia temática, actualidad (priorizando bibliografía de los últimos diez años, salvo documentos clave o fundacionales) y, credibilidad.

Las fases del desarrollo del trabajo se pueden dividir en tres grandes bloques, siendo el primero el Marco Teórico, donde se desarrolla conceptual y contextualmente lo necesario para entender el escenario en el que nos encontramos, seguido del diseño de un protocolo Insider Threat y, por último, un análisis de aplicabilidad como una reflexión crítica sobre la viabilidad de implementar este protocolo en empresas reales del sector tecnológico en España.

Cabe destacar ciertas limitaciones del propio estudio que no han permitido llegar al punto de profundidad óptimo que hubiera gustado:

- No se ha accedido a información interna de empresas reales por razones de confidencialidad. Por esta misma razón, se ha trabajado sin entrevistas ni datos primarios, por lo que el enfoque depende completamente de la literatura disponible.
- El modelo diseñado no se ha validado en un entorno real, dado que el proyecto se basa en una empresa ficticia.

3. MARCO TEÓRICO

3.1. INTRODUCCIÓN A LA SEGURIDAD EMPRESARIAL

Como bien es sabido en la cotidianidad, el trabajo y el esfuerzo que llevamos a cabo a lo largo de nuestra jornada laboral viene motivado por una recompensa final, ya sea el salario, las vacaciones, el reconocimiento o el crecimiento personal, entre tantas. Por lo que, siempre queremos hacerlo bien y darlo todo para disfrutar de estos "premios". Pero, hasta los propios trabajadores, pueden ser los peores enemigos de una empresa.

Entonces, si pongo toda mi dedicación en mi trabajo y creo que estoy en lo correcto, ¿por qué puedo llegar a ser todo lo contrario? Según Cano (2011), la pregunta que deberíamos hacernos es "el ser humano: ¿eslabón más débil o más fuerte de la cadena?".

Los empleados de una organización tienen acceso privilegiado a su información. Por tanto, estos suponen un cortafuegos para cualquier amenaza, pero también una posible preocupación de filtración. Ellos saben el rumbo que toman sus empresas y la confidencialidad de sus informes y su material.

Para Toelle (2021), la compañía debe depositar una confianza en sus trabajadores, pero esta confianza implica riesgos. Un empleado podría romperla de manera negligente al filtrar accidentalmente información confidencial y comunicaciones corporativas. O, en el otro extremo, traicionar esa confianza de manera intencionada, ya sea filtrando, compartiendo o robando propiedad intelectual.

Por ende, *un gran poder conlleva una gran responsabilidad*, y las organizaciones necesitan un protocolo para evitar que las amenazas provengan de fuentes internas y proteger así sus datos sensibles y sistemas digitales de alto valor.

Cubramos todos estos aspectos nombrados anteriormente dentro del concepto de la seguridad empresarial, algo que, para Arroyo Varela (2020), no solo abarca la protección física de las instalaciones y los bienes, sino también la seguridad económica e informacional, ámbitos que están cada vez más interconectados debido a los riesgos del ciberespacio y las amenazas internas. Esta información hace alusión a toda aquella que, en manos equivocadas, podría comprometer la integridad y confidencialidad de la compañía, incluyendo:

- Información confidencial y propiedad intelectual
- Datos de clientes
- Infraestructura tecnológica y recursos humanos, entre otros.

3.1.1. EVOLUCIÓN DE LA SEGURIDAD EMPRESARIAL

Un enfoque reactivo basado en la protección física de activos era el modelo que la seguridad empresarial tenía establecido durante las últimas décadas. Este ha ido evolucionando significativamente hasta llegar a un enfoque integral, incluyendo la gestión de riesgos tecnológicos y humanos. Las organizaciones necesitan implementar modelos proactivos para prevenir amenazas internas, sincronizando sus políticas con normas de seguridad globales (NCSC, 2024).

De acuerdo con Whitelaw et al. (2024), uno de los retos más significativos en la administración de la seguridad empresarial es la adaptación a las nuevas amenazas digitales y el aumento de los ataques internos. Las compañías tecnológicas, específicamente, han sido objeto de situaciones en las que trabajadores desleales han puesto en peligro información vital, lo que subraya la urgencia de establecer tácticas de inteligencia y contrainteligencia en la protección empresarial.

Por otro lado, la cultura organizacional es la que debe enfatizar que esta seguridad corporativa sea parte de ella, promoviendo de esta manera una conciencia de seguridad entre los trabajadores, para así alentar protocolos de supervisión y monitoreo que ayuden a identificar comportamientos sospechosos dentro de la entidad (CoESS, 2019).

En este marco, el próximo apartado abordará las diferencias entre inteligencia, contrainteligencia y seguridad, proporcionando los fundamentos esenciales para comprender el papel de la seguridad empresarial en la protección frente a amenazas internas.

3.2. DIFERENCIAS ENTRE INTELIGENCIA, CONTRAINTELIGENCIA Y SEGURIDAD

Antes de comenzar a profundizar en cada uno de estos conceptos individualmente, es de plena conveniencia revisar lo que nos aporta el Diccionario de la Real Academia Española (RAE) sobre ellos.

- Inteligencia: capacidad de entender o comprender. Capacidad de resolver problemas
- Contrainteligencia (sin. *Contraespionaje*): servicio secreto de un Estado, encargado de la defensa contra el espionaje de naciones extranjeras en su territorio.
- Seguridad: cualidad de seguro. Definiendo *seguro* como libre y exento de riesgo.

La protección de la información y los activos estratégicos de una empresa requieren un enfoque integral que combine estos tres conceptos. Ahora que ya conocemos sus significados tal y como los concibió nuestra lengua, es momento de conocer sus aplicaciones y objetivos dentro de la gestión empresarial (Véase Tabla 1).

Si queremos ser precisos, Toelle (2021) destaca que, en un entorno digitalizado, la seguridad debe incorporar tecnologías avanzadas como la Inteligencia Artificial (IA) y el Machine Learning (ML) para la detección de anomalías en el comportamiento de los empleados. Estas herramientas permiten a las empresas reforzar su capacidad de vigilancia y anticiparse a posibles ataques internos.

LA INTELIGENCIA, CONTRAINTELIGENCIA Y SEGURIDAD EN EL ÁMBITO LABORAL

INTELIGENCIA	Se refiere al proceso de recopilación, análisis e interpretación de información estratégica para la toma de decisiones. En el ámbito empresarial, la inteligencia competitiva permite a las organizaciones anticiparse a tendencias, detectar oportunidades y minimizar riesgos. La inteligencia empresarial no solo se limita a conocer el mercado y la competencia, sino que también abarca el análisis de amenazas internas y externas que pueden comprometer a la seguridad corporativa (Arroyo Varela, 2020; Montoya, 2019).
CONTRAINTELIGENCIA	Se enfoca en la identificación y neutralización de amenazas que puedan comprometer la información crítica de una organización. Su objetivo principal es detectar y prevenir la filtración de datos, el espionaje industrial y las acciones de empleados desleales. La contrainteligencia es una disciplina clave dentro de la seguridad organizacional, ya que permite detectar patrones de comportamiento sospechosos antes de que se conviertan en un riesgo tangible (CoESS, 2019; Díaz Caneja, 2021).

SEGURIDAD	Incluye todas las medidas destinadas a proteger la información, los activos físicos y el capital humano de la empresa. La seguridad empresarial integra tanto la inteligencia como la contrainteligencia para garantizar la resiliencia organizacional ante posibles amenazas. En este sentido, la seguridad no solo se basa en medidas preventivas, sino también en la implementación de controles tecnológicos y en la concienciación de los empleados para reducir el riesgo de incidentes internos (NCSC, 2024; Salman, 2025).

TABLA 1

LA INTELIGENCIA, CONTRAINTELIGENCIA Y SEGURIDAD EN EL ÁMBITO LABORAL

Fuente: *Elaboración Propia a partir de las fuentes citadas en la tabla*

Dejando a un lado los tecnicismos, la relación entre estos tres conceptos es fundamental en la protección de empresas de base tecnológica. Mientras que la inteligencia se centra en obtener información estratégica, la contrainteligencia busca neutralizar las amenazas que puedan derivarse de esa información, y la seguridad establece los protocolos y medidas necesarias para garantizar la integridad de la organización.

Adelantándonos un poco, podemos considerar que el Protocolo Insider Threat actúa como el baricentro del triángulo formado por estos tres elementos, ya que se encuentra en el punto de equilibrio entre la inteligencia, la contrainteligencia y la seguridad. En el siguiente apartado, exploraremos cómo la seguridad de la información se convierte en un pilar fundamental dentro de este esquema.

3.3. LA SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA SEGURIDAD EMPRESARIAL

Este punto se centrará, para su desarrollo, en la norma ISO 27001, para poder comprender los principios de la seguridad de la información.

La ISO 27001 es la certificación encargada de la seguridad y privacidad de la información. En ella se redacta la importancia de los Sistemas de Gestión de Seguridad de la Información (SGSI), siendo un componente esencial de la seguridad empresarial, ya que abarca políticas, procedimientos y controles diseñados para proteger los datos y la infraestructura tecnológica de una organización (AENOR, 2022).

En la era digital, las empresas manejan volúmenes masivos de información y datos sensibles que, de ser comprometidos, pueden causar pérdidas económicas, daños reputacionales y sanciones legales. Es ahí donde entra esta norma y explica perfectamente su crecimiento exponencial en los últimos años.

3.3.1. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Las siglas que nos acompañarán durante esta sección son las conocidas como CIA que, en inglés, hacen referencia a Confidencialidad, Integridad y Disponibilidad (Véase Imagen 1). Estos son los tres principios en los que se fundamenta la seguridad de la información y, juntos, constituyen la base de las estrategias de seguridad en las Tecnologías de la Información (TI) y establecen un marco indispensable para resguardar la información frente a riesgos y posibles brechas.

Veamos que significa cada uno de estos pilares según Beucher (2024):

Confidencialidad

Es el principio que garantiza que los datos solo sean accesibles para personas autorizadas, protegiéndolos contra accesos no autorizados o divulgación indebida. Se aplica tanto a la información digital como física, asegurando la privacidad de individuos y la protección de activos corporativos críticos.

Se pueden añadir también algunos métodos para garantizar esta confidencialidad. Estos son:

- Control de acceso: implementación de autenticación y autorización para limitar el acceso a información sensible.
- Cifrado de datos: aplicación de cifrado en tránsito y en reposo para proteger la información ante posibles ataques.

- Políticas de privacidad y clasificación de datos: definición de protocolos para el manejo adecuado según la sensibilidad de la información (Auditool, 2024).

Integridad

Se refiere a la exactitud y completitud de la información a lo largo de su ciclo de vida, asegurando que no sea alterada de manera no autorizada, ya sea accidental o intencionadamente. Este principio es clave para mantener la confianza en los datos utilizados en la toma de decisiones y operaciones financieras.

Las violaciones a la integridad pueden comprometer la veracidad de la información sin afectar a su confidencialidad, afectando directamente la fiabilidad del sistema. Para evitarlo, se utilizan mecanismos como la verificación de doble factor con firmas digitales y el control de versiones.

Disponibilidad

La disponibilidad garantiza que la información y los sistemas estén accesibles para los usuarios autorizados en el momento en que los necesiten. Es esencial establecer una disponibilidad óptima para evitar interrupciones en las operaciones de una empresa y asegurar la continuidad del negocio en situaciones de emergencia.

IMAGEN 1

PRINCIPIOS CIA

Fuente: *Fortinet (2025)*

Las copias de seguridad periódicas, la revisión de hardware y software para evitar fallos inesperados y distribuir adecuadamente el tráfico de datos, son las estrategias que garantizan esta disponibilidad constante.

Además, Beucher (2024) añade a esta tríada de elementos uno más denominado como autenticidad. Esta confirma el origen legítimo de la información y garantiza que las identidades de los usuarios o entidades involucradas en una transacción o comunicación sean reales y verificadas.

Por lo tanto, queda claro la necesidad de aplicar estos ideales para mitigar cualquier posible riesgo de amenaza interna, ya que los empleados tienen acceso directo a los activos de información de la empresa y, sin controles adecuados, pueden comprometer su seguridad.

3.3.2. AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN

En una batalla lo más común es no llegar a cubrir todos los flancos. Se necesitarían muchísimas herramientas y estrategias de combate para poder estrechar y minimizar las posibilidades de ataques. Pero, en los libros, siempre hay historias de heroicos generales con grandes intelectos capaces de elaborar tácticas para que, en caso de ser atacados, poder defenderse con facilidad.

No puedo decir con exactitud qué resulta más complicado, si ponerse en la piel de ese militar, o tratar de ser una empresa exitosa sin sufrir amenazas de cualquier correspondencia. Lo que sí puedo afirmar es que cuanta más protección tengas, mejor resistirás.

Por consiguiente, debemos pensar en los posibles riesgos que pueden afectar a la seguridad de la información dentro de una organización, entre los cuales destacan:

- Filtración de datos: se refiere a la transmisión no autorizada de información desde el interior de una entidad hacia un destino externo. Esto puede ocurrir tanto de manera intencional como accidental, y puede involucrar tantos medios electrónicos como físicos. Es importante destacar que una filtración no necesariamente implica una acción maliciosa, ya que también puede ser el resultado de un error o descuido por parte de los usuarios internos de la organización (Eckstein, 2015).

- Accesos indebidos de un trabajador: uso no autorizado de sistemas de información, en el que el empleado, motivado por intereses personales o externos, manipula, roba o destruye información crítica.
- Ingeniería social: según López Grande (2015), la ingeniería social se trata del uso de diversas estrategias destinadas a manipular a un usuario con acceso legítimo a los sistemas informáticos de una empresa, con el fin de obtener información confidencial o inducirlo, sin que lo note, a realizar acciones que generen vulnerabilidades en la seguridad. La flaqueza más significativa dentro de una empresa son las personas, y el atacante que emplea estas tácticas lo sabe. Cualquier usuario, ya sean empleados comunes o los mismos encargados, son siempre susceptibles de ser víctimas de este tipo de ataques.

3.3.3. RELACIÓN ENTRE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN INSIDER THREAT

La seguridad de la información y la gestión Insider Threat están estrechamente vinculadas, ya que, como venimos aprendiendo, los empleados y colaboradores con acceso privilegiado a los sistemas de una organización pueden representar un riesgo significativo si no existen controles adecuados. Según Cibersecurity Insiders (2023), el 74% de las organizaciones consideran que las amenazas internas son más difíciles de detectar que los ataques externos, lo que resalta la importancia de elaborar una estrategia al respecto.

Este mismo reporte, al año siguiente liberó unas estadísticas basadas en una encuesta a 467 profesionales de ciberseguridad, revelando tendencias y desafíos notorios en la gestión de amenazas internas. Según esta encuesta, Schulze (2024) extrajo diferentes tendencias:

- El 76% de las organizaciones informaron haber experimentado ataques internos, un incremento respecto al 66% en 2019.
- El 90% de los encuestados considera que los ataques internos son tan difíciles o más difíciles de detectar que los externos.
- Solo un 41% de las empresas han implementado parcialmente programas Insider Threat, dejando en evidencia una falta de monitoreo integral de actividades y estrategias avanzadas para la gestión de amenazas.
- El 29% únicamente considera que cuenta con las herramientas adecuadas para protegerse contra amenazas internas.

La conclusión clara que obtenemos de este estudio es la brecha que existe en las capacidades de seguridad de muchas organizaciones. Pero entonces, ¿qué preguntas debería hacerse una empresa para empezar a resolver estos problemas? (Véase Imagen 2).

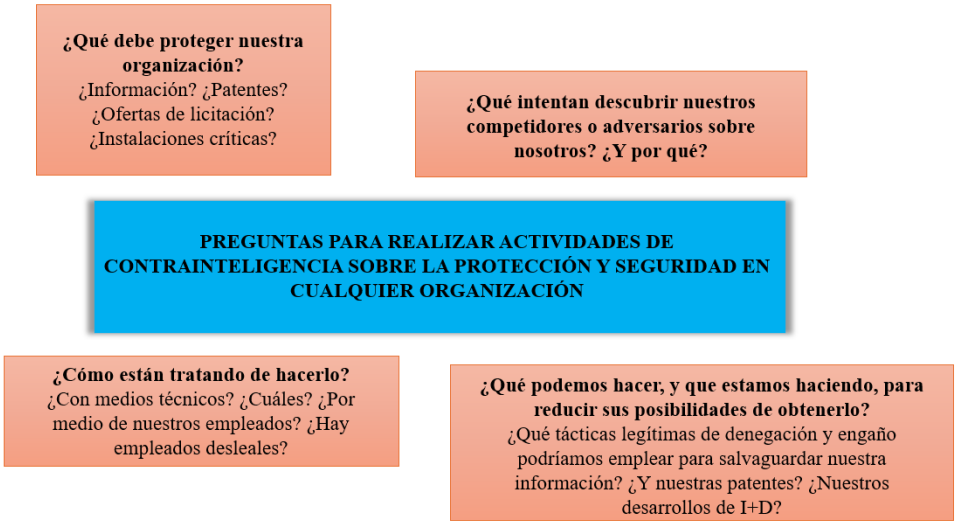


IMAGEN 2

GRUPOS DE PREGUNTAS SOBER LA PROTECCIÓN DE LA INFORMACIÓN Y DEL CONOCIMIENTO DE UNA ORGANIZACIÓN

Fuente: *Elaboración propia a partir de Díaz Caneja (2021)*

Estas preguntas no sirven de nada si no se trata de remediar. En los últimos cinco años, las empresas se han dado cuenta que las amenazas internas son tan difíciles o incluso más difíciles de identificar y prevenir que las externas. Es cierto que la encuesta refleja una mayor conciencia sobre la complejidad y discreción con la que operan las amenazas internas, pero sabemos que estas presentan desafíos únicos para su detección, ya que involucran a usuarios legítimos que aprovechan su acceso y profundo conocimiento de la organización para evadir controles de seguridad (Schulze, 2024).

En consecuencia, para hacer frente a esta dificultad, son necesarias soluciones de seguridad avanzadas que permitan una mayor visibilidad sobre el comportamiento de los usuarios y sus actividades.

Usted que está leyendo esta memoria, sabrá que más adelante se creará un protocolo Insider Threat específico para estas amenazas. Si bien venimos mostrando el camino adecuado a seguir, acabaremos dando todas las directrices necesarias para su elaboración, pero mientras tanto, Schulze (2024) las resume en varias actividades:

- Análisis del comportamiento
- Monitoreo inteligente para identificar incluso las señales más sutiles
- Fomento de una cultura de seguridad dentro de la empresa
- Enfoque de seguridad en capas, combinando controles técnicos y administrativos

3.3.4. LA CONTRAINTELIGENCIA COMO HERRAMIENTA EN LA PREVENCIÓN DEL INSIDER THREAT

Ya conocemos que la contrainteligencia es una disciplina fundamental y, según Vilas Rodríguez (2017), esta es una herramienta crucial para la defensa de empresas y organizaciones frente a actores internos que puedan comprometer su integridad.

La contrainteligencia debe enfocarse en el control del personal, asegurando que quienes manejan información estratégica sean personas de confianza. Para ello, desarrollemos un concepto denominado la "política de necesidad de saber" (Lowenthal, 2006 *apud* Vilas Rodríguez, 2011).

Esta política, unida a la compartimentación de la información, son unas prácticas que limitan el acceso de los empleados únicamente a los datos que necesitan conocer para desempeñar su labor.

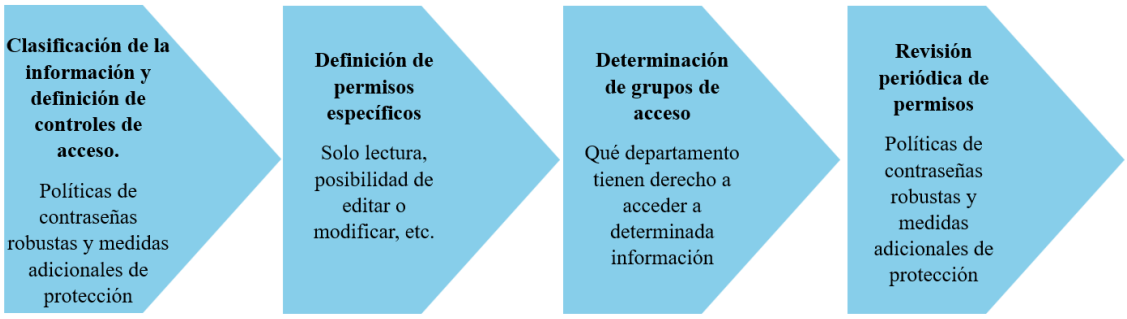


IMAGEN 3

PAUTAS CLAVE PARA UNA POLÍTICA NEED TO KNOW EFICIENTE

Fuente: *Elaboración propia a partir de González (2022)*

Para González (2022), el principio que él llama *Need-to-Know*, es necesario para evitar riesgos relacionados con filtraciones de datos internas o eliminación de información

sensible, así como otras acciones que podrían comprometer los procesos de negocio. Para aplicarlo de manera efectiva, el primer paso es definir una política de control de acceso que establezca claramente qué información debe ser protegida dentro de la empresa, seguido del proceso de establecer quién accede a qué datos y con qué permisos.

Es así como la Imagen 3 hace referencia al procedimiento que debe seguirse si se quiere aplicar esta política de manera correcta y hacer un buen uso de ella.

3.4. INSIDER THREAT: DEFINICIÓN Y TIPOLOGÍA

A diferencia de las amenazas externas, las internas son particularmente desafiantes debido al conocimiento profundo que estos actores tienen sobre la organización y sus sistemas. Tras este entrenamiento para conocer un poco el contexto que gira en torno al Insider Threat, es momento de adentrarnos en el concepto que gira en torno a este proyecto y ponerle nombre y apellidos. Hagámoslo fácil:

A lo largo de los años, se han proporcionado distintas definiciones para el término de *insider*. Una buena descripción podría ser: "aquel individuo que es empleado (pasado o presente), contratista u otro tercero de confianza, que tiene acceso privilegiado a las redes, sistemas o datos de una organización" (Nurse et al, 2014).

3.4.1. CLASIFICACIÓN DE LOS TIPOS DE INSIDERS

Dentro del estudio de las amenazas internas, es fundamental comprender que no todas se manifiestan de la misma forma. En términos generales, pueden clasificarse en dos grandes categorías: los *insiders maliciosos* y los *insiders no maliciosos o accidentales*.

Definámoslos para comprender cómo son estos individuos y su manera de actuar, a partir de Inayat et al (2024) y Nurse et al (2014):

3.4.1.1. INSIDERS MALICIOSOS

El individuo con acceso privilegiado actúa de manera intencionada con el fin de dañar la confidencialidad, integridad o disponibilidad de la información, sistemas o infraestructura

de la organización. La motivación detrás de estas acciones puede ser económica, personal, ideológica o de venganza.

Las formas de ataque perpetradas por estos insiders pueden ser muy variadas y de diferente gravedad, incluyendo:

- Brechas de datos: divulgación no autorizada de información confidencial.
- Sabotaje: uso de código malicioso, destrucción de hardware o sistemas para perjudicar la operativa.
- Filtración de datos: ya sea mediante credenciales, dispositivos USB o técnicas avanzadas.
- Ataques basados en credenciales: robo o uso indebido de contraseñas para obtener acceso elevado.
- Espionaje: recolección encubierta de información estratégica.
- Fraudes y estafas: manipulación de datos, informes falsos, uso indebido de información personal.
- Suplantación de identidad (masquerading): actuar fingiendo ser un usuario autorizado distinto.

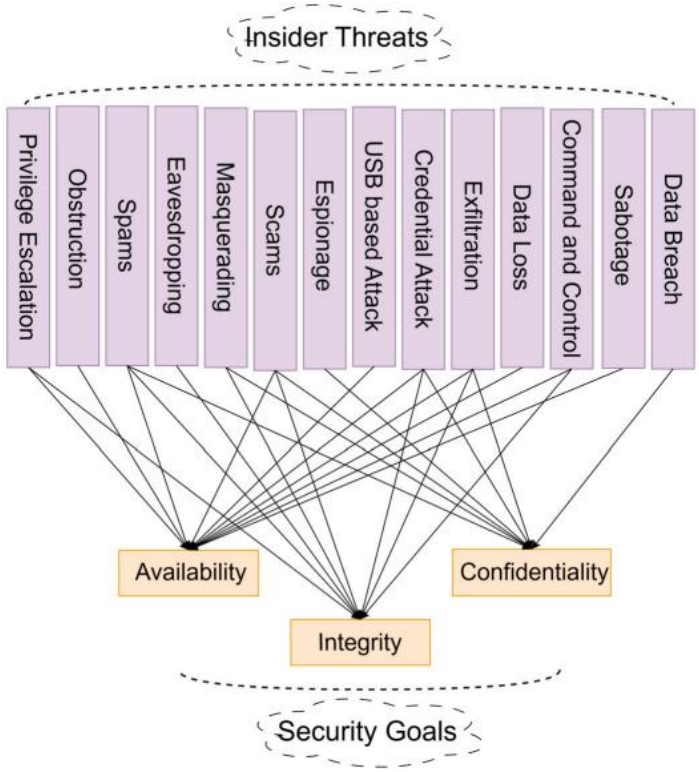


IMAGEN 4

FORMAS DE ATAQUE DE LOS INSIDERS MALICIOSOS

Fuente: *Inayat et al (2024)*

Otros menos comunes podrían ser la escucha clandestina (eavesdropping), el spam y pérdida de datos deliberada, la obstrucción y la escalada de privilegios, siendo esta el acceso no autorizado a funciones restringidas del sistema.

La Imagen 4 sirve como resumen de todas estas formas que tienen los insiders maliciosos de actuar y, como se puede comprobar, hace alusión a Confidencialidad, Integridad y Disponibilidad (CIA), conceptos que desarrollamos anteriormente y que, sin ellos, sería muy difícil abordar estos peligros.

3.4.1.2. INSIDER NO MALICIOSO O ACCIDENTAL

Contrario al anterior, el insider accidental no tiene intenciones dañinas, pero su conducta puede comprometer igualmente los activos de la organización. De hecho, esta es considerada la forma más común de amenaza interna.

En este caso, el daño se produce por errores humanos, negligencia, desconocimiento o mal diseño de los sistemas. Esto incluye acciones u omisiones que generan consecuencias como:

- Pérdida de dispositivos de trabajo, como ordenadores o móviles con datos corporativos.
- Publicación accidental de información sensible en redes sociales.
- Caída en ataques de phishing u otras campañas de malware disfrazado.
- Configuraciones incorrectas o prácticas inseguras por falta de formación.

A pesar de su carácter no malicioso, estos comportamientos aumentan la probabilidad de sufrir una brecha de seguridad y deben ser gestionados con el mismo rigor que las amenazas intencionadas.

3.5. LA PSICOLOGÍA DETRÁS DEL INSIDER THREAT

El insider threat no es solo un problema técnico o estructural dentro de las organizaciones. En realidad, el aspecto más impredecible y, a la vez, más crucial, es el factor humano. Por eso, el estudio de la psicología de los insiders se ha convertido en un campo emergente y esencial en la seguridad organizacional. Ruohonen & Saddiqa (2024), llevan a cabo una revisión sistemática que muestra cómo, a pesar de su creciente interés, la psicología

de las amenazas internas sigue siendo un campo con muchos vacíos tanto teóricos como empíricos. Veamos, por tanto, algunas teorías explicativas del comportamiento insider a lo largo del siguiente punto, basadas en los autores nombrados anteriormente.

3.5.1. TEORÍAS EXPLICATIVAS DEL COMPORTAMIENTO INSIDER

Un crimen ocurre cuando se juntan dos factores: un motivo y una oportunidad. Esta es conocida como la teoría de la Prevención Situacional del Delito (SCP, por sus siglas en inglés). Entonces, esta sería desmontada fácilmente si eliminamos uno de estos dos elementos de la ecuación.

En nuestro contexto, podemos traducirlo en empleados con accesos privilegiados que encuentran la posibilidad de actuar, especialmente cuando no existen suficientes controles técnicos y administrativos. Para reducir el riesgo de un ataque malicioso, Ruohonen & Saddiqa (2024) aseguran que bastaría con "contraatacar" a través de monitorizaciones rigurosas de inicios de sesión y accesos, mientras que la oportunidad podría disminuir si se instalan procedimientos de autorización más estrictos y de doble autenticación.

Esta teoría nos lleva a otra denominada como la Teoría de la Disuasión General (GDT, por sus siglas en inglés). Los delincuentes toman decisiones sopesando los beneficios de sus acciones frente a los costes que conllevan, como las sanciones. Para aumentar estos costes, las organizaciones deben implementar mecanismos de disuasión como la formación y la concienciación, que informen a los empleados sobre las consecuencias de un comportamiento inadecuado (Ruohonen & Saddiqa, 2024).

La disuasión se fundamenta principalmente en factores externos, como las sanciones o recompensas monetarias por un buen desempeño, pero también hay que considerar los factores intrínsecos (Lee et al, 2023). La motivación, que se refiere al deseo de actuar correctamente sin esperar recompensas externas, puede verse afectada por aspectos como la insatisfacción laboral, lo que a su vez debilita el cumplimiento voluntario de las políticas de seguridad.

Además, todas estas teorías van de la mano de la teoría de la elección racional, que sostiene que los delitos se cometen de manera deliberada, con la clara intención de obtener una recompensa, ya sea económica, material, de prestigio o simplemente por emoción. Esta perspectiva se refleja en modelos como el de la Imagen 5, el Triángulo o Diamante del Fraude, que identifican tres componentes claves: motivo (o presión), oportunidad y racionalización. Esta última se refiere al proceso mental mediante el cual los infractores justifican sus acciones.

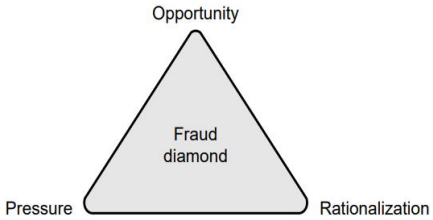


IMAGEN 5

TRIÁNGULO DEL FRAUDE

Fuente: Ruohonen & Saddiqa (2024)

Por ejemplo, un insider con deudas podría justificar su conducta diciendo que necesita pagar sus cuentas. Incluso aquellos insiders que no tienen malas intenciones pueden racionalizar su comportamiento, como compartir contraseñas, al pensar que no es una infracción grave.

Para contrarrestar este tipo de racionalizaciones, las organizaciones deben contar con políticas claras sobre seguridad, conducta ética, propiedad intelectual y secretos comerciales, además de implementar mecanismos de control y refuerzo.

Existen numerosas teorías más que complementan a las ya citadas, como la teoría de la acción razonada y la teoría del comportamiento planificado, donde se explican cómo las actitudes y el control conductual percibido influyen en las intenciones de conducta (Ruohonen & Saddiqa, 2024).

3.5.2. CARACTERÍSTICAS PERSONALES Y CIRCUNSTANCIAS DEL INDIVIDUO

El comportamiento insider no puede entenderse sin considerar la interacción entre dos dimensiones clave: las características personales estables del individuo y las circunstancias que atraviesa en el tiempo. Ambas influyen de forma decisiva en la

propensión a cometer una acción lesiva hacia la organización, ya sea de forma maliciosa o negligente (Ruohonen & Saddiqa, 2024).

En lo que respecta a las circunstancias personales, la literatura identifica diversos factores desencadenantes (*trigger factors* o *precipitating events*) que actúan como presión y pueden motivar una acción desleal. Estos incluyen:

- Problemas financieros, adicciones o vicios.
- Conflictos familiares o situaciones personales inestables.
- Despidos, no renovaciones de contrato o cambios organizativos negativos, como reasignaciones forzosas o reducción de salario.
- Falta de reconocimiento profesional, evaluaciones negativas o advertencias disciplinarias (Ruohonen & Saddiqa, 2024; Lee et al., 2023).

MONEY (DINERO)	No hay forma mejor de obtener información confidencial que mediante el soborno. Es uno de los métodos de reclutamiento más efectivos.
IDEOLOGY (IDEOLOGÍA)	Se aprovecha de un conflicto filosófico que el empleado tiene con los métodos de su organización, o bien de su lealtad hacia gobiernos o causas extranjeras
COMPROMISE (COMPROMISO/ CHANTAJE)	A través de la extorsión, se amenaza con revelar información personal o profesional perjudicial para forzar al objetivo a colaborar
EGO	Se explota la baja autoestima o el resentimiento de empleados que se sienten menospreciados. Esto puede alimentarse con fantasías de espionaje o el deseo de ser reconocidos. Un ejemplo clásico es el de un empleado de un subcontratista de Grumman Aircraft Corporation, que entregó planos del sistema de radar F-14 a la KGB porque se sentía ignorado. Esta tecnología fue copiada e instalada en el caza soviético MIG-29

TABLA 2

MNEMOTECNICA “MICE”

Fuente: *Elaboración Propia a partir de* Vashisth & Kumar (2013)

Estos factores están precisamente alineados con el Triángulo del Fraude, específicamente con el componente "presión". Asimismo, Vashisth & Kumar (2013) añaden un concepto denominado MICE (por sus siglas en inglés: *Money, Ideology, Compromise, Ego*). Este principio, tradicionalmente utilizado en la comunidad de inteligencia, indica que la mayor parte de los espías actúan guiados por alguno de estos cuatro elementos mostrados en la Tabla 2.

Según Ruohonen & Saddiqa (2024), está demostrado que ciertos perfiles contractuales y laborales pueden asociarse a mayor riesgo. Por ejemplo, se ha observado que empleados con contratos a tiempo parcial, próximos a su finalización y en situaciones de deuda, presentan una combinación propicia para desencadenar conductas insider. Además, afirman que existen características personales más estables que también constituyen al riesgo:

- Curiosidad, ansias de exploración y alto conocimiento sobre las políticas de seguridad para la facilitación del acceso indebido o acciones no éticas.
- Aislamiento social o trabajo remoto, asociados a la menor supervisión y conexión emocional con la organización, erosionando el sentido de lealtad corporativa.
- La jerarquía en la empresa también se destaca, siendo los empleados con posiciones de alta responsabilidad los que tienen una tendencia mayor a cometer alguna infracción.

3.5.2.1. BIG FIVE (OCEAN)

Si queremos hablar de los rasgos de personalidad, debemos comenzar por uno de los marcos más utilizados en la evaluación del riesgo de insider threat. Este es el modelo de los cinco grandes rasgos de personalidad (*Big Five*) que se reflejan en la Tabla 3.

Los estudios muestran que los empleados con baja responsabilidad y alto neuroticismo tienden a cometer más errores o actos negligentes, mientras que aquellos con alta apertura pueden buscar desafíos que impliquen evadir controles de seguridad. En contextos organizacionales, estos rasgos deben ser evaluados con herramientas psicométricas fiables, como el cuestionario CSEC (Cybersecurity Questionnaire), que permite identificar perfiles de riesgo en base a patrones de comportamiento digital (Schoenherr & Thomson, 2021).

OPENNESS (APERTURA A LA EXPERIENCIA)	Se refiere a la creatividad, la curiosidad intelectual y la disposición de aceptar nuevas ideas. Tener un alto nivel en este rasgo puede estar relacionado con una mayor exploración del entorno digital y, en algunos casos, con el deseo de acceder a información restringida simplemente por interés o curiosidad
CONSCIENTIOUSNESS (RESPONSABILIDAD)	Es el autocontrol y el cumplimiento de las normas. Este rasgo es uno de los más importantes en el ámbito de la seguridad de la información, ya que una puntuación baja se ha vinculado a una mayor tendencia a violar políticas de seguridad, como compartir contraseñas o ignorar protocolos
EXTRAVERSION (EXTRAVERSIÓN)	Está relacionada con la sociabilidad y la necesidad de estímulo externo. Aunque su papel en el comportamiento insider es un poco más complicado, niveles altos de extraversión pueden afectar cómo un individuo interactúa con sus compañeros y su visibilidad dentro de la organización
AGREEABLENESS (AMABILIDAD)	Indica la tendencia a ser cooperativo y compasivo. Un bajo nivel de amabilidad se ha asociado con una menor disposición a seguir reglas o a considerar cómo nuestras acciones afectan a los demás, lo que puede llevar a comportamientos más egoístas o manipuladores.
NEUROTICISMO (NEURITICISM)	Refleja la estabilidad emocional. Un alto nivel de neuroticismo está relacionado con la ansiedad, la inestabilidad emocional y la dificultad para manejar el estrés, lo que puede hacer que una persona reaccione de manera desproporcionada ante situaciones de presión organizacional

TABLA 3

BIG FIVE (OCEAN)

Fuente: *Elaboración Propia a partir de Ruohonen & Saddiqa (2024) y Schoenherr & Thomson (2021)*

3.5.2.2. LA TRÍADA OSCURA DE LA PERSONALIDAD

Otro conjunto de rasgos ampliamente estudiado en nuestro ámbito es el denominado como la Tríada Oscura. Con los testimonios de González Moraga (2015) y Barrutieta & Ursúa (2011) podemos definir muy bien los tres conceptos que la componen. Estos son:

- Maquiavelismo: como una estrategia interpersonal que aboga por los propios intereses, el engaño y la manipulación.
- Narcisismo subclínico: falta de afecto en las relaciones interpersonales, falta de preocupación por los demás, ausencia psicopatológica importante y bajo compromiso ideológico.
- Psicopatía subclínica: insensibilidad afectiva, manipulación interpersonal y ausencia de remordimientos.

Ruohonen & Saddiqa (2024) proponen ejemplo para cada elemento de esta tríada. Las personas con altos niveles de maquiavelismo tienden a instrumentalizar a otros para sus propios fines, lo que las hace peligrosas si tienen acceso privilegiado a información sensible.

Por otro lado, los narcisistas pueden justificar el robo de información por creer que están subvalorados o que merecen un reconocimiento que la organización no les proporciona. Y, por último, la psicopatía puede estar asociada a un desprecio por las normas y una mayor probabilidad de actuar sin considerar las consecuencias.

Entonces, es lógico decir que la presencia de uno o varios de estos rasgos en un individuo no implica por sí sola la certeza de una amenaza, pero sí aumenta su propensión al comportamiento insider, especialmente cuando se combina con factores de presión o una cultura organizacional débil.

Pese a su utilidad, Ruohonen & Saddiqa (2024) advierten que estos rasgos deben utilizarse con precaución y que los motivos de los insiders no son estáticos. Un empleado puede ver crecer o disminuir su satisfacción laboral, su compromiso con la empresa o su sentido de justicia organizacional a lo largo del tiempo. Esto implica que la probabilidad de convertirse en amenaza también puede fluctuar. Por tanto, entender la evolución de estas variables es clave para prevenir la deslealtad futura.

4. DISEÑO DEL PROTOCOLO INSIDER THREAT

Como era de esperar, antes de comenzar con el desarrollo de nuestro protocolo, es necesario contextualizar el mundo empresarial en el que nos vamos a mover, las características de la organización que se ha seleccionado y su descripción y situación específica para poder entender la importancia y el móvil de este proyecto. Para que el proceso sea más llevadero, se le asignará un nombre y una caracterización ficticia a la empresa:

ESTUDIO DE CASO: Cynerdata Solutions, S.L es una empresa de base tecnológica con domicilio en Málaga, especializada en el desarrollo de soluciones avanzadas e inteligencia artificial y big data aplicadas a la ciberseguridad empresarial. Desde sus inicios en 2018, ha experimentado un crecimiento exponencial hasta consolidarse como un referente nacional en el sector TIC, especialmente en el ámbito del software como servicio (SaaS) orientado a sectores críticos como la banca, la energía y la industria aseguradora.

Su producto principal es CynerGuard, una plataforma SaaS que combina detección temprana de amenazas, análisis predictivo mediante Machine Learning y automatización de respuestas ante incidentes. Este servicio, que requiere una manipulación constante de datos altamente sensibles, hace que la protección de la información se convierta en una necesidad estratégica.

Actualmente, la organización cuenta con 180 trabajadores divididos en distintos departamentos: I+D y desarrollo de software, seguridad informática, atención al cliente, legal, RRHH y dirección general. El modelo de trabajo se podría catalogar como híbrido, ya que el 50% del tiempo se trabaja de forma presencial y la otra mitad, en remoto.

Como se puede comprender, su activo más importante es la información, y su manejo puede llegar a ser crítico. Entre esta información se encuentran:

- *Modelos de inteligencia artificial entrenados con datos de clientes*
- *Informes confidenciales sobre vulnerabilidades detectadas en los sistemas de los clientes*
- *Documentación contractual, licencias de software y acuerdos de confidencialidad*
- *Código fuente propio*
- *Datos personales y laborales de sus empleados*

En este contexto, las amenazas internas representan uno de los principales desafíos para la organización. La posibilidad de que un empleado con acceso legítimo pueda actuar de forma maliciosa, negligente o ser manipulado por agentes externos supone un riesgo real para la continuidad del negocio y la reputación de la compañía.

4.1.FUNDAMENTOS DEL PROTOCOLO Y VISIÓN ESTRATÉGICA

Si queremos crear un protocolo eficaz contra amenazas internas, este debe sustentarse en una serie de principios fundamentales que estructuren su funcionamiento y garanticen su efectividad. Mylrea et al. (2018) proponen un marco metodológico adaptado al contexto organizacional, integrando la gestión de amenazas complejas en los sistemas de una empresa:

La prevención de amenazas internas exige más que un conjunto de controles de seguridad: requiere una arquitectura estratégica basada en principios sólidos que guíen el diseño, implementación y mejora continua del protocolo.

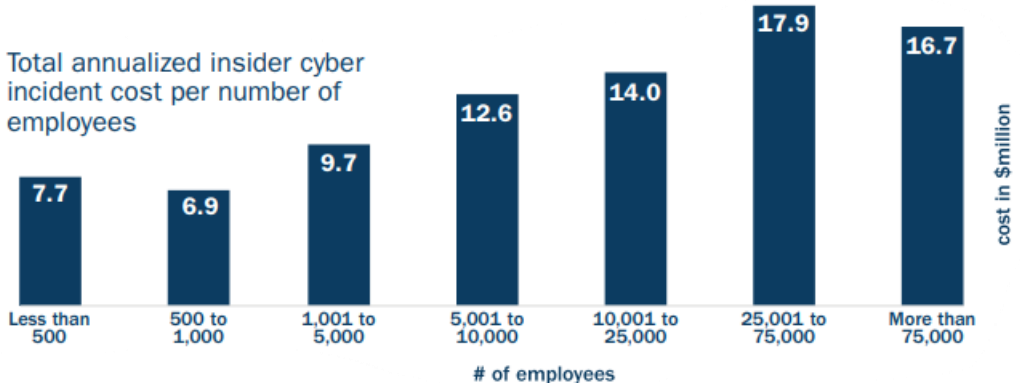
El primer objetivo de cualquier programa contra insiders es prevenir que estas ocurran. ¿Qué implica esto? Implementar medidas que reduzcan la posibilidad de que un empleado, colaborador o contratista se convierta en una amenaza. En este sentido, la prevención abarca desde la contratación segura (todo tipo de *background checks*, entrevistas conductuales, etc.), hasta políticas de acceso basadas en el principio de mínimo privilegio y separación de funciones (SEI, 2022).

Centrémonos en los principios y pilares en los que se apoyará el protocolo para poder comprender la importancia y la complejidad que este conlleva.

4.1.1. PRINCIPIO DE GESTIÓN DEL RIESGO Y RESILIENCIA ORGANIZACIONAL

El protocolo se sustenta sobre una base de análisis de riesgos, entendiendo que cada amenaza interna potencial debe evaluarse en función de su probabilidad de ocurrencia y su impacto sobre los activos críticos. En línea con el enfoque CISA (2020) y el modelo de Mylrea et al. (2018), se propone una arquitectura basada en:

- Identificación y clasificación de activos críticos (código fuente, datos de clientes, etc.)
- Evaluación continua del riesgo con herramientas dinámicas y dashboards interactivos.
- Inclusión de métricas para evaluar exposición, vulnerabilidad y capacidad de respuesta.



GRÁFICA 1

COSTE DE LOS INCIDENTES ANUALES POR INSIDERS SEGÚN NÚMERO DE EMPLEADOS

Fuente: *CISA (2020)*

Como muestra la Gráfica 1, el coste medio anual por incidentes relacionados con insiders se incrementa significativamente con el tamaño de la empresa. Aunque Cynerdata Solutions se encuentra en el rango de menos de 500 empleados, la alta criticidad de sus activos hace que el impacto pueda ser proporcionalmente mayor. Este dato refuerza la necesidad de implementar un protocolo basado en la gestión proactiva del riesgo.

La Imagen 6 ilustra la intersección de tres factores clave: criticidad, vulnerabilidad y amenaza. Su combinación permite evaluar el riesgo desde una perspectiva combinada. En nuestro contexto, la imagen facilita la identificación de escenarios críticos: por ejemplo, un empleado del área de desarrollo con acceso a modelos de IA (activo crítico), que presenta señales de insatisfacción laboral (vulnerabilidad) y cuyo rol permite el acceso remoto sin supervisión directa (amenaza).

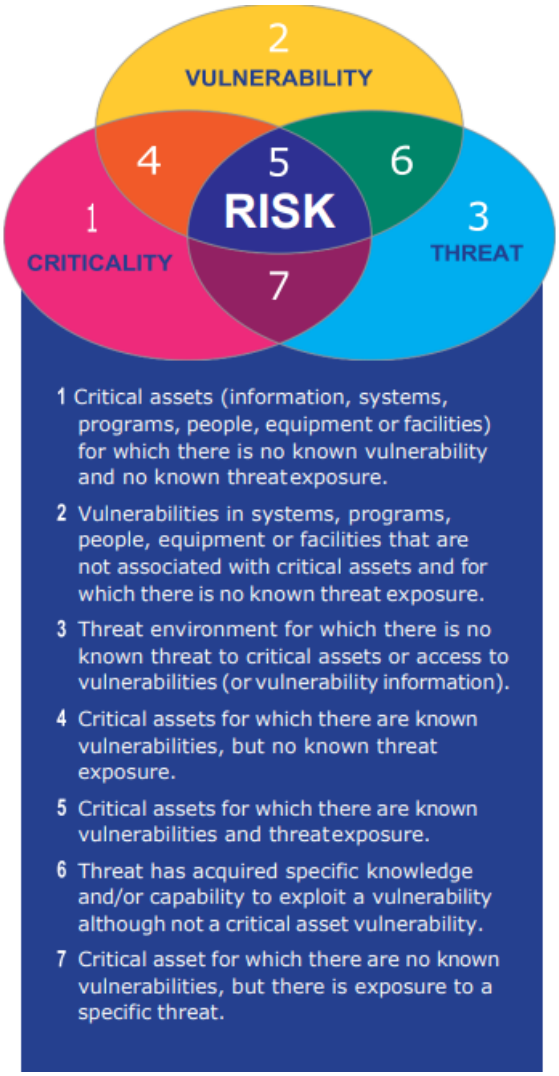


IMAGEN 6

RISK MODEL

Fuente: *SIFMA (2024)*

4.1.2. PRINCIPIO DE DEFENSA EN PROFUNDIDAD Y REDUNDANCIA

Este principio, aplicado a raíz del modelo SEI (2022) y Mylrea et al. (2018), establece la importancia del diseño ciberfísico adaptado a una defensa por capas, incluyendo controles técnicos, siendo estos firewalls, controles de acceso según atributos, etc.; controles administrativos, como separación de funciones y registros de logs; y, controles físicos como videovigilancia.

Esta triple arquitectura permite una tolerancia a fallos más robusta y aumenta la capacidad de detección y contención temprana de incidentes internos.

4.1.3. PRINCIPIO DE ENFOQUE CENTRADO EN LAS PERSONAS

Según Mylrea et al. (2018), el insider no debe ser visto únicamente como actor malicioso, sino también como vector de oportunidad de mejora. Por ello, el protocolo pone énfasis en la dimensión humana mediante:

- Formación continua y gamificación de riesgos
- Canales de denuncia seguros y confidenciales
- Programas de bienestar psicosocial y seguimiento de señales conductuales
- Evaluación del clima organizacional como indicador predictivo (CISA, 2020)

4.1.4. PRINCIPIO DE LEGALIDAD, PROPORCIONALIDAD Y TRANSPARENCIA

Toda arquitectura debe ser ética, verificable y orientada a proteger tanto a sistemas como personas. Por tanto, el modelo SIFMA (2024) desarrolla la necesidad de cumplir estrictamente con estas premisas.

IMAGEN 7

OBLIGACIONES DE LA EMPRESA Y DERECHOS DEL EMPLEADO

Fuente: *Elaboración con IA a partir de SIFMA (2024)*

Además, se impone una vigilancia interna ética sobre el uso de herramientas de monitorización digital para asegurar que el tratamiento de datos se rige por principios de necesidad y minimización, que toda medida es auditada y justificada antes posibles revisiones y, que se mantiene un equilibrio entre control organizacional y derechos del trabajador.

Entonces, como señala la Imagen 7, el reto del protocolo Insider Threat consiste en encontrar el equilibrio adecuado entre las obligaciones legales de la empresa de proteger los sistemas y activos de esta, y el derecho del trabajador a no ser sometido a una vigilancia abusiva o desproporcionada. La clave está en políticas claras, consentimiento informado y asesoramiento legal constante.

4.1.5. PRINCIPIO DE CULTURA DE SEGURIDAD E INTELIGENCIA COLECTIVA

Finalmente, el protocolo se apoya en el desarrollo de una cultura preventiva, horizontal y participativa, donde la seguridad se entiende como un valor compartido y no como un sistema impositivo. Este principio, según el modelo CISA (2020), se traduce en:

- Integración de la ciberseguridad en la estrategia corporativa
- Incentivos al reporte de incidentes y a la mejora continua
- Inspiración en el enfoque de correlación de nodos y análisis contextual de red como proponen Mylrea et al. (2018), planteando un marco que permite avanzar hacia esquemas de inteligencia, distribuida en la detección colaborativa de amenazas internas.

Como resumen y de manera visual, se proporciona la Tabla 4 para entender de un vistazo los pilares en los que se apoyará el resto del protocolo, para así asegurar su coherencia estratégica, su viabilidad operativa y su legitimidad ética dentro de la organización:

Principio fundamental	Aplicación en Cynerdata Solutions
Gestión del riesgo y resiliencia organizacional	Priorización de activos, dashboards de riesgo, continuidad operativa

Defensa en profundidad y redundancia	Controles técnicos, administrativos y físicos superpuestos
Enfoque centrado en las personas	Formación, canal de denuncia, clima laboral, seguimiento psicosocial
Legalidad, proporcionalidad y transparencia	Auditoría legal del protocolo, documentación, protección de derechos
Cultura de seguridad e inteligencia colectiva	Cultura de seguridad, inteligencia distribuida, liderazgo activo

TABLA 4

RESUMEN DE LOS PRINCIPIOS DEL PROTOCOLO INSIDER THREAT

Fuente: *Elaboración Propia*

5. MODELOS DE REFERENCIA PARA LA DETECCIÓN Y MITIGACIÓN DEL INSIDER THREAT

Sirva este punto como antesala metodológica, a razón de aportar profundidad conceptual. Se presentarán varios marcos comparados, siendo estas distintas maneras de enfocar un programa Insider Threat, para más tarde justificar la creación del protocolo propio para Cynerdata Solutions.

5.1. APLICACIÓN DE LOS "7 CORE STEPS" DEL MODELO SIFMA

No había mejor modelo para establecer un punto de partida estructural que el ofrecido por SIFMA (2024). El enfoque indexa siete pasos clave hacia la implementación de un programa efectivo de protección contra insiders:

1. Priorizar y delimitar alcance: la empresa debe definir los objetivos para su protocolo Insider Threat, así como sus prioridades a nivel organizacional y su tolerancia asociada al riesgo.
2. Orientar: se identifican los activos vulnerables, el marco normativo y las amenazas hacia la entidad.

3. Evaluar el estado actual: se revisan las medidas existentes de seguridad lógica, acceso remoto, etc., detectando las posibles carencias.
4. Realizar un análisis de riesgos: se valora la probabilidad e impacto de eventos maliciosos o negligentes.
5. Diseñar un estado objetivo: se desarrolla un estado futuro para el programa.
6. Identificar y priorizar las brechas: se compara el estado actual con el objetivo de determinar posibles brechas y se crea un plan de acción prioritario para abordarlas. El objetivo es realizar un análisis de coste/beneficio y un entendimiento del riesgo que conlleva.
7. Ejecutar el plan de acción: se definen las acciones de mitigación y se monitorean las practicas que se estén llevando a cabo.

Gracias a esta estructura, podemos otorgar un enfoque de mejora continua basado en la evaluación, implementación y retroalimentación cíclica.

5.2. MARCO IPDRR

Uno de los marcos más ampliamente adoptados para estructurar la ciberseguridad organizacional es el IPDRR, haciendo alusión a sus siglas en inglés: *Identify, Protect, Detect, Respond* y *Recover*. Este modelo se ha integrado en muchos protocolos reales a pesar de que su enfoque original fue más generalista, tal y como se describe en el informe de SIFMA (2024) y Mylrea et al. (2018). Es por ello por lo que, en base a estos autores, describiremos el funcionamiento de este programa:

IMAGEN 8

MODELO IPDRR

Fuente: *Mylrea et al. (2018)*

5.2.1. IDENTIFY

Se trata de una fase estratégica, ya que permite establecer una línea base de exposición que luego servirá para priorizar recursos y esfuerzos. Esta función busca identificar los activos, procesos y personas críticas dentro de la organización. Se divide en categorías como: gestión de activos, gobernanza y gestión del riesgo. Existen diferentes tareas, entre las cuales podemos encontrar:

- Realizar inventario de activos críticos
- Establecer un mapa de roles y accesos: quién accede a qué y en qué condiciones
- Definir el perfil de terceros y socios estratégicos, cuya colaboración podría suponer un riesgo
- Documentar las políticas y procedimientos de gobernanza interna del programa
- Comunicación al personal de la existencia del protocolo, así como la incorporación de un entrenamiento de sensibilización.
- Acuerdos de confidencialidad (por ejemplo: qué se puede hablar online a través de redes sociales).
- El proceso comienza desde que se contrata al empleado y sigue por su monitoreo. Se debe responder ante comportamientos sospechosos o disruptivos.

5.2.2. PROTECT

Protect hace alusión al desarrollo e implementación de salvaguardas que aseguren el funcionamiento de los activos y minimicen la probabilidad de un incidente causado por un insider. Podríamos dividirlo en las siguientes categorías:

- Controles de acceso: repasar activamente los privilegios de los empleados, revisar periódicamente las bases de la configuración de los sistemas de la empresa, contar con un procedimiento *off-boarding* (asegurar que cuando un empleado abandone la entidad, toda la información quede ahí, incluyendo: terminación de acceso físico y electrónico, cambiar las contraseñas de los sistemas a los que el empleado tenía acceso, etc.).
- Conciencia y entrenamiento: asegurar que el personal recibe el entrenamiento adecuado, así como la actualización en materias relevantes, incluyendo: protocolos para manejar la información sensible, hacer responsables a los empleados para alertar

si detectan alguna actividad sospechosa o inusual y, básicamente, establecer unos estándares mínimos de seguridad educacional.

- Información, Protección y Procedimientos: las políticas y procesos de la organización deben estar a salvo ante cualquier posible amenaza interna, por lo tanto, es de debido cumplimiento tener una documentación y unos controles adecuados, un *backup data* y una cultura de trabajo que mida el éxito basado en métricas dedicadas al ambiente y el clima laboral apropiados.

5.2.3. DETECT

En este eje se concentra el esfuerzo de observación, análisis y diagnóstico por medios como:

- Uso de tecnologías de detección de anomalías
- Establecimiento de canales de reporte confidencial
- Monitorización activa de logs, accesos remotos y cambios de privilegios
- Mantenimiento de la moral de los empleados, creando un proceso disciplinario justo, para evitar que cualquier persona con intenciones de crear una amenaza contra la empresa, sepa las consecuencias y considere no actuar de manera malintencionada.

5.2.4. RESPOND

Esta función está diseñada para contener y gestionar el incidente una vez detectado, desde procedimientos de investigación hasta el desarrollo de un proceso de desvinculación de empleados. Es necesario seguir estos pasos, indicados en la Tabla 5:

COMUNICACIÓN	El comienzo debe estar en conducir una investigación que cubra: - La revisión de los sistemas afectados - La interrogación de los sospechosos y testigos - La documentación de las evidencias - La creación de un árbol de decisiones que se base en: intervenir o seguir monitorizando el comportamiento que nos concierne, cuándo implicar al personal capacitado en insiders, qué circunstancias justifican la consulta con

	expertos externos y qué situaciones requieren notificar a las fuerzas del orden.
ANÁLISIS	Determinar si el incidente fue intencionado o no y, a partir de ahí, implementar herramientas para detectar cualquier anomalía en los programas y documentos. Además, es importante conocer qué tipo de ataque ha sido y hacia qué, es decir, si ha afectado a la información organizacional o no.
MITIGACIÓN	Erradicar toda vulnerabilidad en la seguridad que pueda afectar en el futuro, así como decidir qué acción legal debe ser tomada contra la persona responsable y crear un proceso de terminación inmediata de la empresa para desvincular totalmente a dicho insider.

TABLA 5
PASOS DE LA FUNCIÓN "RESPOND"
Fuente: SIFMA (2024)

5.2.5. RECOVER

Por último, Recover se centra en restaurar la operatividad, aprender del incidente y reforzar la resiliencia organizativa mediante:

- Evaluación del incidente: reunirse con el personal apropiado para incluir mejoras para prevenir incidentes similares en el futuro
- Comunicación de actividades de recuperación y aviso de cambios en las políticas de la empresa
- Inclusión del incidente en los informes de la empresa y, según lo exijan las obligaciones regulatorias, informar de este a las autoridades estatales.
- Aplicación de protocolos de restauración segura de datos

En conclusión, el modelo IPDRR facilita una cobertura integral que no solo se enfoca en prevenir ataques, sino en detectar y responder a tiempo, con un enfoque resiliente y adecuado a la legalidad. Esto permite integrar aspectos técnicos, humanos y organizativos para que de verdad sirva como solución efectiva en caso de sufrir una amenaza interna dentro de la empresa.

5.3. MODELO CISA SOBRE LOS ELEMENTOS CLAVE PARA UN PROTOCOLO INSIDER THREAT EXITOSO

La guía de mitigación de amenazas internas de CISA (2020) propone una aproximación integral para enfrentar el insider threat, siendo esta una visión especialmente útil identificada en diez elementos clave que deben estar presentes en cualquier programa de mitigación eficaz:

1. Alineación con la cultura y misión de la organización. El programa debe estar integrado en la identidad organizativa, en lugar de percibirse como una estructura ajena o de control sancionador.
2. Identificación de activos críticos. Mapear aquellos elementos cuya pérdida o compromiso supondría un impacto grave para la empresa.
3. Definición de amenazas internas significativas. Se debe partir de escenarios realistas y basados en la experiencia, como el uso negligente de accesos remotos, sabotaje por insatisfacción laboral, etc.
4. Capacidad para detectar indicadores de amenaza. Desarrollar mecanismos que recojan señales tempranas de diversas fuentes: logs, cambios de conducta, canales de reporte internos, etc.
5. Procedimientos de respuesta ante incidentes. No basta con detectar, hay que tener protocolos de actuación bien definidos.
6. Participación de stakeholders. Todas las áreas funcionales de la empresa deben tener voz y voto en la gestión del caso.
7. Promoción de cultura del reporte. Una organización que no escucha a tiempo es una organización más vulnerable.
8. *Hub* de análisis centralizado. La información dispersa pierde valor. Es necesario consolidar la información clave en un nodo de inteligencia, donde se analicen patrones, se detecten correlaciones y se organicen las alertas.
9. Equipo de gestión de amenazas internas. Su función es analizar, valorar y actuar ante los casos detectados. Este equipo debe contar con perfiles complementarios (técnicos, legales, psicológicos).
10. Programa de formación y concienciación. La prevención efectiva solo es posible si el personal está capacitado y sensibilizado. Esto implica formación continua y métricas que permitan medir el impacto.

5.4. MODELOS TEÓRICOS ADICIONALES

Además de los marcos técnicos comentados anteriormente, se ofrecen modelos complementarios que enriquecen la comprensión del insider threat desde una perspectiva interdisciplinar. Estos enfoques teóricos son de gran utilidad para contextualizar los riesgos en empresas con entornos complejos

5.4.1. ROUTINE ACTIVITY THEORY

En el punto 3.5.1. ya dijimos que un crimen ocurre cuando se juntan dos factores: un motivo y una oportunidad. Pues bien, la Routine Activity Theory (RAT), se basa en la premisa de que la comisión de un delito (en este caso, amenaza interna), requiere la coincidencia de tres elementos clave: un actor motivado, un objetivo vulnerable o atractivo y la ausencia de guardianes eficaces (Shaikh & Oliveira, 2019; Clifton, 2024).

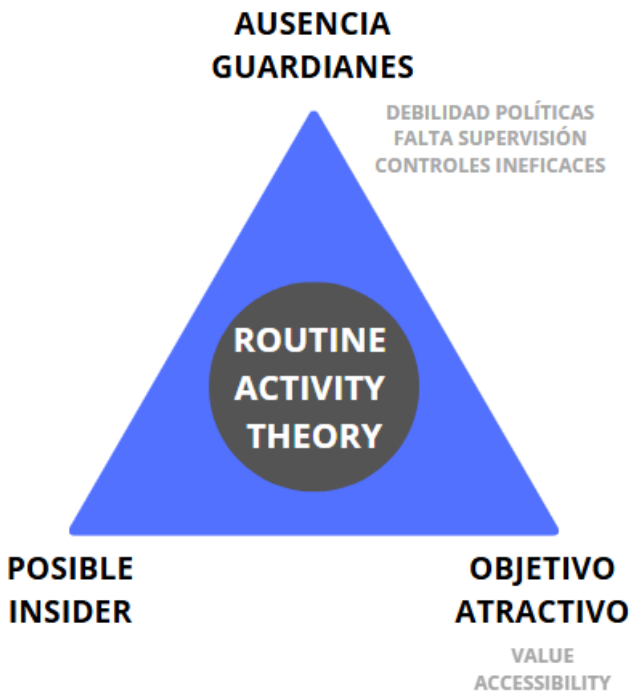


IMAGEN 9

ROUTINE ACTIVIY THEORY

Fuente: *Elaboración Propia a partir de* Shaikh & Oliveira (2019)

Este enfoque ha sido recientemente adoptado por el ámbito de la seguridad de los sistemas de información para explicar cómo ciertos entornos organizacionales (especialmente aquellos marcados por el uso de las tecnologías informales o *Shadow IT*) pueden facilitar comportamientos que comprometen la integridad de los activos digitales (Clifton, 2024).

El estudio de Shaikh & Oliveira (2019), adapta RAT al contexto del insider threat derivado del uso de tecnologías informales (por ejemplo, uso no autorizado de apps como Dropbox o Google Docs en el entorno laboral). En este marco, el riesgo no proviene únicamente de la intención maliciosa, sino del uso rutinario de tecnología fuera del control institucional, lo que genera oportunidades para desviaciones, negligencias o abusos no intencionados.

Se destacan dos variables críticas del modelo (Shaikh & Oliveira, 2029):

- *Value* (valor del objetivo): cuanto más valiosa es la información, más atractivo resulta el objetivo para el posible infractor.
- *Accessibility* (accesibilidad): cuanto mayor es la facilidad del acceso, más aumenta la probabilidad de ocurrencia.

La ausencia de guardianes (entendida como debilidad en las políticas, falta de supervisión, controles técnicos ineficaces o ausencia de cultura del cumplimiento), completa el triángulo del riesgo, como se puede observar en la Imagen 9.

Entonces, RAT se consolida como un marco predictivo y preventivo útil para analizar la seguridad de la información en entornos tecnológicos digitalizados.

5.4.2. ENFOQUE SOCIOTÉCNICO

La estrategia sociotécnica adoptada por la mitigación de riesgos internos comienza por la base de que “seguridad” no se puede entender ni gestionar desde un marco meramente tecnológico. Por el contrario, exige aproximación integral que considere tanto los sistemas técnicos (hardware, software, redes) como las facetas sociales y humanas (comportamientos, relaciones laborales, cultura de las empresas) que cohabitan y se influyen entre sí dentro de las empresas (Clifton, 2024; Mujinca et al., 2017).

Según Mujinca et al. (2017), este enfoque tiene en cuenta que los sistemas organizativos constituyen una red de experiencias de interrelación entre sujetos, tecnologías y estructuras institucionales y, que se podrá proteger únicamente contra amenazas internas de aquellos que se orienten en sus medidas técnicas, en relación coherente con las relaciones humanas internas. Para ello, la amenaza interna ha de entenderse como vulnerabilidad emergente del propio sistema sociotécnico y no únicamente en función de un riesgo individual o tecnológico.

Se ha hecho evidente la relevancia de utilizar estrategias sociotécnicas compuestas (*stacked socio-technical strategies*) dentro de un modelo de defensa en profundidad. Dichas estrategias combinan herramientas técnicas con políticas organizativas para fomentar el buen comportamiento del empleado durante su carrera en la empresa, facilitando captar desviaciones significativas en relación con patrones normales de actividad (Mujinca et al., 2017).

Como indica Clifton (2024), este enfoque se puede consolidar con la adopción de ontologías empleadas en ciberseguridad que incorporen tanto los acontecimientos técnicos como humanos. Estas, se utilizan en las tareas de estructurar y clasificar los indicadores de amenaza de tal manera que se puedan emplear de referencia en sistemas de detección temprana y análisis automatizado.

Por ello, no es sólo relevante, sino necesario. Facilita ir más allá de las consideraciones técnicas puras y comprender cómo las prácticas en las organizaciones, las relaciones humanas y las condiciones de trabajo comparten (o no comparten) el proceso de crear entornos seguros. Además, favorece un entorno de corresponsabilidad en el que todos los trabajadores, y no sólo el personal técnico, tienen un papel activo en las medidas de previsión frente a incidentes.

Por lo tanto, a modo de transición, tras haber analizado en detalle los principales modelos de referencia en la detección y mitigación de amenazas internas, se cuenta con una base metodológica y conceptual sólida sobre la que construir una propuesta propia.

A continuación, se presenta el diseño de un protocolo Insider Threat adaptado específicamente a la realidad organizativa, tecnológica y cultural de Cynerdata Solutions, teniendo en cuenta sus activos críticos, su modelo híbrido de trabajo y el nivel de exposición al riesgo derivado del tipo de información que maneja. Este protocolo busca integrar las

mejorar prácticas internacionales con un enfoque personalizado, alineado con la misión estratégica de la empresa.

6. DISEÑO DEL PROTOCOLO INSIDER THREAT PARA CYNERDATA SOLUTIONS S.L

Tal y como ya habíamos adelantado, el diseño de un protocolo frente a amenazas internas representa una herramienta esencial para prevenir, detectar y mitigar incidentes provocados por personas con acceso legítimo a los activos críticos de una organización.

En el caso de Cynerdata Solutions S.L, empresa tecnológica que desarrolla soluciones basadas en inteligencia artificial y big data aplicadas a la ciberseguridad, la gestión del riesgo insider adquiere una especial relevancia debido a la sensibilidad de los datos que maneja: algoritmos de IA entrenados, informes de vulnerabilidades, contratos confidenciales, código fuente y datos personales de empleados y clientes.

Este protocolo se ha diseñado siguiendo los principios de gestión de riesgos que se desarrollaron en el punto 5 de la memoria. Se ha optado por una estructura adaptable y escalable, teniendo en cuenta la dimensión media de la empresa (180 empleados) y su modelo híbrido de trabajo.

En cuanto a los objetivos que busca cumplir este modelo, se podrían plasmar de la siguiente manera:

- Proteger la confidencialidad, integridad y disponibilidad de los activos digitales e intelectuales de la empresa.
- Prevenir filtraciones, sabotajes, espionaje y otros actos maliciosos o negligentes cometidos por insiders.
- Detectar de manera temprana comportamientos anómalos o indicios de riesgo.
- Establecer respuestas ágiles, proporcionadas y respetuosas con los derechos laborales y la privacidad.
- Fomentar una cultura organizativa basada en la confianza, la prevención y la corresponsabilidad.

6.1. COMPONENTES DEL PROTOCOLO INSIDER THREAT

El diseño de un protocolo efectivo para la gestión de amenazas internas requiere una estructura modular, coherente y adaptada al ciclo de vida de la amenaza. Siguiente las recomendaciones de Kont et al. (2015) (Modelo CCDCOE de la OTAN), Ali et Al. (2017) y Cappelli et al. (2012) (CERT Guide to Insider Threats), se identifican una serie de componentes esenciales para articular un sistema integral de prevención, detección y respuesta ante comportamientos anómalos o maliciosos por parte de empleados o colaboradores con acceso autorizado.

Este apartado desarrolla dichos componentes, adaptado al contexto específico de nuestra empresa en cuestión. Cada componente responde a una función crítica dentro del sistema: desde la gobernanza y la definición de responsabilidades hasta los mecanismos de monitorización mediante inteligencia artificial, pasando por políticas de formación, control de acceso y evaluación del programa.

6.1.1. GOBERNANZA Y ESTRUCTURA ORGANIZATIVA

La base de todo protocolo requiere una estructura de gobernanza sólida. Esta debe estar alineada con los principios de la organización, abarcar funciones interdepartamentales y contar con el respaldo de la alta dirección. Como destaca CISA (2020), “los programas de mitigación de amenazas internas son de naturaleza multidisciplinaria y, dado que se intersecan con múltiples funciones empresariales, requieren patrocinio y compromiso a nivel ejecutivo”.

Para ello, se recomienda establecer un Grupo de Gestión de Amenazas Internas con representantes de áreas clave como Seguridad de la Información, Recursos Humanos (RRHH), Asesoría Jurídica, Dirección General y Compliance. Esta recomendación está en línea con los principios de la Guía del NCSC (2024), que indica que los departamentos deben constituir un grupo de trabajo con representantes de todas las oficinas interesadas, cuya actividad les sitúe en posición de recibir información relevante sobre el comportamiento de los empleados.

Asimismo, la *Fact Sheet* de CISA (2024) señala que “las organizaciones deben formar un equipo de gestión de amenazas multidisciplinario para crear un plan de respuesta

a incidentes, de modo que se garantice que su respuesta esté estandarizada y se pueda aplicar y repetir de manera consistente"

En este marco, se establecen los siguientes roles dentro del equipo de gobernanza, apoyados en CISA (2020):

- Responsable del programa Insider Threat: será la figura designada por la alta dirección como autoridad ejecutiva del protocolo. Su función principal es coordinar las políticas, representar al programa ante la gerencia y supervisar las operaciones estratégicas del equipo.
- Oficial de RRHH: encargado de gestionar los aspectos psicosociales, apoyar en la detección de señales de alertas conductuales y, coordinar los procedimientos de incorporación y salida del personal.
- Representante legal/compliance: garantiza que el protocolo se aplique respetando la legalidad vigente, la proporcionalidad de las medidas y la protección de los derechos laborales.
- Responsable de seguridad (CISO): evalúa riesgos técnicos, lidera los procesos de monitorización y protección de activos, y coordina las herramientas tecnológicas asociadas.
- Coordinador de formación y cultura preventiva: lidera programas de concienciación, formación continua y campañas de cultura de seguridad.

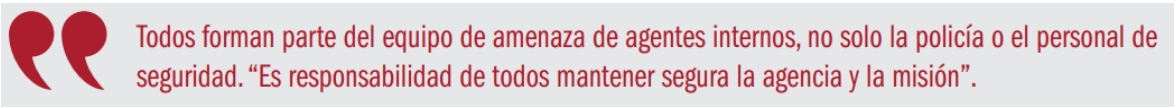


IMAGEN 10

CITA SOBRE LA GOBERNANZA EN UN PROTOCOLO INSIDER THREAT

Fuente: *CISA (2024)*

Esta estructura debe contar con una política formal publicada y comunicada a toda la organización (CISA, 2020). Además, tal y como refleja la Imagen 10, la gobernanza del programa debe facilitar la coordinación interdepartamental, la toma de decisiones basada en el riesgo, y el equilibrio entre seguridad organizacional y respeto por las libertadas de cada trabajador. Si esta estuviera mal definida o sin apoyo de la dirección general, constituiría uno de los principales factores de fracaso de este tipo de programas (CISA, 2024).

6.1.2. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS CRÍTICOS

"Uno no sabe lo que tiene hasta que lo pierde". No existe mejor expresión popular que refleje con más claridad la realidad de muchas organizaciones que, tras sufrir una filtración de información o un incidente de seguridad, descubren demasiado tarde qué activos eran realmente esenciales para su funcionamiento.

Un buen protocolo Insider Threat exige, como paso inicial e ineludible, conocer a fondo qué se posee, qué se debe proteger y qué se está poniendo en riesgo si no se actúa con previsión. Tal y como indica CISA (2024), las organizaciones deben identificar "lo que valoran y sus activos físicos e intelectuales críticos para protegerse contra amenazas de agentes internos".

Este proceso debe permitir a la organización reconocer, clasificar y proteger aquellos activos cuya exposición, alteración o pérdida podría poner en riesgo su misión, reputación o viabilidad. Por tanto, el núcleo de un programa eficaz reside en contar con un proceso para identificar, rastrear y monitorizar los activos críticos de la organización (CISA, 2020).

Se recomienda adoptar un enfoque basado en servicios, que parte de identificar los procesos clave de negocio y sus servicios asociados, descendiendo jerárquicamente hasta los activos que los sustentan (SEI, 2022). Este tipo de inventario permite mapear con precisión los elementos imprescindibles para la empresa.

Una vez inventariados los activos, deben clasificarse en función de los siguientes criterios:

- Impacto en la misión empresarial
- Coste de reposición o pérdida
- Accesibilidad (nivel de privilegio requerido)
- Requisitos regulatorios o legales asociados
- Frecuencia de uso o interacción

SEI (2022) también recomienda emplear metodologías como el Pairwise Ranking, que permite realizar comparaciones sistemáticas entre activos para determinar su relevancia relativa de forma objetiva y sin riesgos. Además, CISA (2020) propone mantener una base de datos estructurada de activos críticos que incluya, al menos, la siguiente información: tipo de activo, ubicación, nivel de clasificación del riesgo, uso principal, personas con acceso autorizado, procedimiento de acceso y revocación y coste estimado en caso de pérdida.

Estos criterios cobran aún más relevancia si se consideran los datos de la Imagen 11, donde se señala que los tipos de información más susceptibles a ataques internos son: los datos financieros, de clientes, de empleados, propiedad intelectual, configuraciones del sistema, credenciales de acceso, etc.

IMAGEN 11

DATOS MÁS SUSCEPTIBLES DE ATAQUES INSIDER

Fuente: Schulze (2024)

Entonces, es momento de poner en contexto esta información para aplicarla a Cynerdata Solutions. Los activos más críticos que se han identificado en la empresa incluyen:

- Algoritmos de IA entrenados (propiedad intelectual estratégica)
- Código fuente del software principal: la plataforma CynerGuard
- Informes técnicos sobre vulnerabilidades y amenazas emergentes
- Datos personales de empleados, clientes y proveedores
- Contratos confidenciales y documentación legal
- Accesos a entornos de desarrollo y producción

Todos estos activos, denominados por CISA (2020) como las *Crown Jewels* (joyas de la corona), deben estar incluidos en un registro unificado, mantenido y supervisado por el responsable de seguridad, de manera que se permita una correcta trazabilidad y asignación de responsables.

6.1.3. EVALUACIÓN DE VULNERABILIDADES Y AMENAZAS INTERNAS

Vamos a darle a Cynerdata Solutions un enfoque multidimensional para implementarlo en este apartado del protocolo. Con este, podrá anticiparse a posibles amenazas internas, evaluarlas con rigor y activar intervenciones proporcionales antes de que se materialicen en incidentes de impacto.

Evaluar una vulnerabilidad no implica simplemente identificar fallos técnicos, va más allá: requiere comprender los perfiles de los posibles atacantes, sus motivaciones, patrones de comportamiento y el contexto organizativo que puede facilitar la aparición de conductas perjudiciales.

6.1.3.1. EVALUACIÓN BASADA EN PERFILES DE AMENAZA

Kont et al. (2015), en el marco CCDCOE de la OTAN, plasman una evaluación basada en perfiles de amenaza, es decir, categorías definidas en función de las motivaciones, medios, momentos y objetivos que caracterizan a diferentes tipos de atacantes internos, basados en casos documentados. Se identifican cuatro perfiles principales:

- *IT Sabotage*: ejecutado principalmente por empleados técnicos con acceso privilegiado. Su motivación más común es la venganza, y suelen atacar los sistemas que previamente gestionaban, a menudo tras la notificación de despido.
- Robo de Propiedad Intelectual: aquellos empleados que tienen acceso a información sensible, como los ingenieros. El robo suele ocurrir dentro de los sesenta días antes o después de abandonar la organización, y está motivado por el deseo de emprender un nuevo negocio, llevarse la información a un nuevo puesto, o incluso cederla a terceros externos.
- Fraude: asociado a trabajadores de nivel medio o bajo que, impulsados por necesidad financiera o codicia, manipulan procesos internos o sustraen información personal identificable. Este tipo de amenaza suele desarrollarse durante largos períodos y puede implicar a cómplices dentro o fuera de la organización.
- Espionaje: ataques motivados por múltiples causas (económicas, ideológicas, políticas), que pueden permanecer latentes durante años y manifestarse en acciones específicas muy planificadas.
- Además, se incluyen los insiders no maliciosos o no intencionados.

Estos perfiles permiten a Cynerdata Solutions anticipar escenarios de riesgos según el contexto de cada empleado y su función. Por ejemplo:

- Un desarrollador con acceso a código crítico y que ha manifestado su intención de dejar la empresa podría encajar en el perfil de robo de propiedad intelectual.
- Un técnico de sistemas sancionado podría representar riesgo de sabotaje si mantiene accesos privilegiados.
- Un administrativo con problemas financieros podría suponer un vector de fraude continuado.

Por lo tanto, incorporar esta lógica al sistema de evaluación y detección del programa, permitirá priorizar recursos, ajustar medidas de supervisión y diseñar respuestas específicas según el tipo de perfil.

Estos perfiles se pueden ajustar según la clasificación que aportan Inayat et al. (2024), una clasificación avanzada de tipos de insiders basada en el tipo de acceso, intencionalidad y objetivos de la amenaza: turncloaks (empleados que atacan por venganza), lone wolves (actúan por cuenta propia), security evaders (mezcla de descuido y engaño) y contracted insiders (agentes externos infiltrados).

6.1.3.2. FACTORES DE RIESGO PERSONALES Y ORGANIZACIONALES

La evaluación de vulnerabilidades no puede limitarse al análisis técnico: debe incluir las dimensiones personales, psicológicas y organizacionales que pueden motivar o facilitar una conducta maliciosa. Como señalan Kont et al. (2015), los incidentes relacionados con amenazas internas suelen tener sus raíces en problemas personales no visibles para los sistemas técnicos, pero sí observables por compañeros, supervisores o responsables de RRHH.

La Imagen 12 muestra como los factores personales pueden tener un efecto directo en la predisposición de un empleado a actuar de forma negligente o maliciosa. La depresión, las rupturas afectivas, los fallecimientos cercanos o los despidos inminentes se correlacionan con cada uno de los perfiles de amenaza nombrados en el punto 6.1.3.1.

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Depression	High	Low	Low	Medium	High
Financial obligations	Low	High	High	Medium	Low
Address change (moving)	Low	High	High	Medium	Medium
Death among family or friends	Medium	Medium	Low	Medium	High
Feelings of inadequacy	High	Medium	Low	High	Medium
Break-up or divorce	Medium	Low	Low	Medium	High
Impending termination of contract	High	High	Low	Medium	Medium

IMAGEN 12

DATOS MÁS SUSCEPTIBLES DE ATAQUES INSIDER

Fuente: Kont et al. (2015)

Además, factores como el abuso de sustancias, el aislamiento social o conflictos previos con la organización son señalados por CISA (2020) como señales de alerta que, acumuladas, pueden aumentar significativamente el riesgo. Estas circunstancias son personales, y no existe ningún protocolo institucional para comunicarlas y que la empresa esté al tanto. Sin embargo, el personal de RRHH o tus propios compañeros podrían identificar señales tempranas si se cuenta con una cultura de seguridad proactiva.

Por otro lado, no todas las amenazas provienen de factores individuales. El entorno laboral puede amplificar el riesgo cuando actúa como desencadenante. CISA (2020) advierte de entornos con las siguientes características: falta de reconocimiento, injusticias reales o percibidas, ambientes tóxicos o jerárquicos cerrados, ausencia de procesos para canalizar quejas, aplicación incoherente de sanciones, falta de formación o procesos de evaluación inexistentes.

Estas condiciones pueden erosionar la cultura organizacional, incrementar el resentimiento y facilitar el pensamiento de conductas maliciosas. La interacción de estos factores con las vulnerabilidades personales es la que convierte a un empleado corriente en un insider.

Finalmente, si queremos tener un enfoque más técnico y cuantificable, Alsowail & Al-Shehari (2021), proponen utilizar instrumentos psicométricos para detectar niveles de estrés, predisposición al conflicto y disonancia moral. Entre ellos destacan un modelo basado en la *Workplace Deviance Scale* (WDS) y herramientas como el Cyber-Criminal Intent and Stress Level Questionnaire (CCISLQ), que evalúan variables como el grado de justificación

moral del delito, la percepción de impunidad, la influencia de su entorno personal (familia, amigos, compañeros) y el nivel de estrés acumulado y soporte emocional disponible.

Estas métricas permiten asignar niveles de riesgo (bajo, medio, alto) a empleados, no para sancionarlos, sino para anticipar contextos de riesgo y reforzar medidas preventivas.

6.1.4. MEDIDAS PREVENTIVAS Y DE DISUASIÓN

Un insider no puede prevenirse exclusivamente con tecnología. Su mitigación requiere una combinación equilibrada de controles técnicos, políticas organizativas, gestión de accesos y, sobre todo, cultura preventiva. Tal y como afirma CISA (2020), "una organización resiliente se construye desde la integración de la concienciación, los controles y la conducta segura".

Una de las medidas más efectivas de prevención es invertir en concienciación del personal. La formación regular sobre amenazas internas, phishing, uso aceptable de los recursos, custodia de los datos sensibles o canales de denuncia, es imprescindible. Todos los empleados que manejan información sensible deben recibir formación inicial en sus primeros treinta días y actualizaciones anuales posteriores (NCSC, 2024).

Inayat et al (2024) proponen incluir campañas prácticas como simulaciones de phishing, seguimiento del comportamiento de respuesta y análisis posterior de las vulnerabilidades humanas detectadas.

Por otra parte, los privilegios de acceso deben estar estrictamente alineados con las funciones del empleado. Clifton (2024) señala que una de las causas más comunes de incidentes internos es el exceso de accesos no justificados, muchas veces nunca revisados tras cambios de puesto, proyectos o salidas del personal.

Por lo tanto, el máximo exponente en esta situación sería la integración del principio de mínimo privilegio (SEI, 2022): cada usuario debe tener únicamente el nivel de acceso estrictamente necesario para desempeñar sus funciones. Esta medida, que se ha consolidado como estándar de seguridad, ayuda a contener daños de accesos indebidos o cuentas comprometidas.

En paralelo, el modelo *Zero Trust Architecture* (ZTA), está ganando fuerza como paradigma de referencia en la ciberseguridad moderna. Tal y como define Burke (2024),

Zero Trust es “un enfoque de gestión del riesgo que no confía en ningún dispositivo, archivo o configuración a menos que haya sido verificado y autorizado correctamente para conectarse, ejecutarse o implementarse en el sistema”.

Este enfoque rompe con la lógica clásica del “perímetro de confianza” y se apoya en tres principios fundamentales:

1. No confiar por defecto en ningún usuario, dispositivo o conexión, incluso dentro de la red corporativa.
2. Verificación continua de la identidad, integridad y contexto de cada solicitud de acceso.
3. Aplicación estricta del mínimo privilegio, restringiendo accesos, incluso temporales o indirectos.

Cynerdata Solutions utiliza el entorno Windows y, según Burke (2024), implementar ZTA en estos entornos reduce el riesgo de infecciones por malware, escaladas de privilegios y exfiltraciones de datos ante ataques internos o externos. En particular, ZTA es eficaz contra vectores como phishing o uso indebido de credenciales, que suelen estar implicados en un gran porcentaje de brechas internas.

Aunando estos conceptos, podemos aplicarlos para nuestra empresa: Cynerdata Solutions cuenta con una cultura de seguridad distribuida y especializada, donde cada nuevo empleado recibe una formación inicial de seguridad centrada en la protección de propiedad intelectual, gestión ética de datos y control de accesos.

Además, por poner un ejemplo claro, los desarrolladores acceden solo a entornos de prueba o producción según su función específica, siguiendo el esquema del mínimo privilegio. Las claves y accesos temporales se generan y destruyen automáticamente tras su uso con herramientas como Hashicorp, plataforma de gestión de secretos organizacionales (de Diego, 2025).

Otros procesos y políticas adecuadas a la empresa son:

- Las actualizaciones del protocolo Insider Threat se comunican trimestralmente y los trabajadores con acceso a datos críticos firman acuerdos de confidencialidad reforzados, también aplicables a colaboradores externos y becarios
- El equipo de RRHH colabora con el resto de los trabajadores para detectar cambios de comportamiento, estrés laboral o conflictos personales.

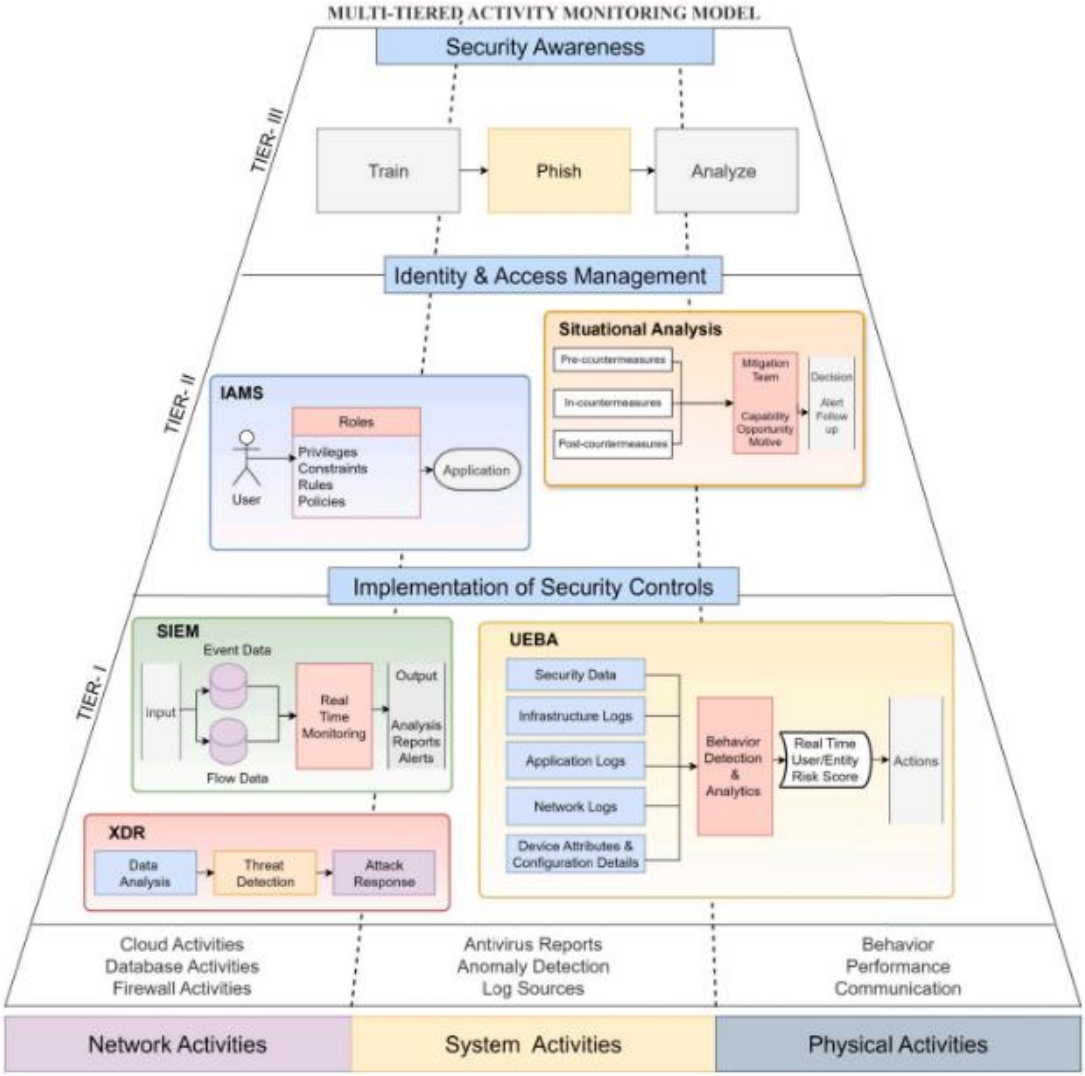
- Los accesos a información confidencial son auditados en tiempo real mediante sistemas como UEBA (explicado en el próximo punto), y se activa un protocolo de revisión ante eventos fuera de patrón (por ejemplo: acceso masivo a repositorios o filtración de dispositivos extraíbles).
- Todo empleado que deja la empresa debe desprenderse automáticamente de credenciales y accesos, y su comportamiento digital de las últimas semanas es auditado. Además, se le realiza una entrevista final donde se analiza su percepción de la organización y se advierte expresamente de las cláusulas de propiedad intelectual post-contractual.

6.1.5. MONITORIZACIÓN Y DETECCIÓN DE COMPORTAMIENTOS ANÓMALOS

La detección temprana de amenazas internas en Cynerdata Solutions requiere un sistema de monitorización robusto, que combine la recopilación masiva de datos con análisis inteligentes de comportamiento. El modelo más completo y aplicable al contexto de nuestra empresa es el *Multi-Tiered Activity Monitoring Model* propuesto por Inayat et al. (2024), que organiza la defensa en tres niveles complementarios, como se puede ver en la Imagen 13.

TIER I – Implementación de controles de seguridad: incluye soluciones como SIEM (*Security Information and Event Management*), UEBA, (*User Entity Behavior Analytics*) y XDR (*Extended Detection and Response*):

- SIEM: permite correlacionar eventos y generar alertas en tiempo real a partir de logs del sistema, red de dispositivos y aplicaciones. Es eficaz para detectar patrones ya conocidos o sospechosos.
- UEBA: va un paso más allá. Utiliza aprendizaje automático para modelar el comportamiento habitual de cada usuario y detectar desviaciones anómalas, incluso si el usuario está correctamente autenticado. Además, Wang & El Saddik (2023) añaden que UEBA "asocial el comportamiento de usuarios y entidades con patrones históricos, detectando riesgos nuevos o desconocidos (*unknown unknowns*) que los métodos tradicionales no pueden identificar".
- XDR: integra diferentes fuentes (red, correo, nube) para ofrecer una visión unificada del riesgo, facilitando el trabajo del CISO al combinar eventos de múltiples canales.



MAGEN 13

MULTI-TIERED ACTIVITY MONITORING MODEL

Fuente: Inayat et al. (2024)

TIER II – Gestión de identidad y acceso: utiliza plataformas IAMS (*Identity and Access Management Systems*) para vincular accesos, permisos y roles con riesgos específicos. Se complementa con análisis de contexto, historial y función del usuario.

TIER III – Concienciación de seguridad: incluye actividades como simulaciones de phishing, formación periódica y análisis de respuesta para reforzar la resiliencia humana ante amenazas internas, tanto intencionadas como accidentales.

Siendo así la descripción de esta arquitectura, implementémosla para Cynerdata Solutions:

TIER I:

- Se ha configurado un motor UEBA que modela la actividad normal de cada empleado y alerta ante accesos a repositorios en horas no habituales, patrones de copia de datos no autorizados o navegación web anómala.
- Se han desplegado herramientas SIEM para recopilar eventos de seguridad desde endpoints, accesos remotos y servidores de producción.
- XDR se utiliza para relacionar amenazas entre los sistemas locales y la infraestructura cloud (donde se encuentran los módulos de IA y bases de datos sensibles).

TIER II:

- El sistema IAM automatiza la asignación y revocación de permisos según el puesto y ciclo de vida del empleado.
- Se realiza análisis situacional en contextos de cambio de rol, fricciones laborales o intentos de salida voluntaria, con verificación por parte de todos los departamentos.

TIER III:

- Se ejecutan campañas semestrales de concienciación con simulacros de phishing dirigidos, evaluaciones post-formación y retroalimentación.
- El personal firma anualmente un código ético y de seguridad digital, reforzado con comunicaciones trimestrales sobre actualizaciones del protocolo.

6.1.6. RESPUESTA ANTE INCIDENTES

La eficacia de un protocolo Insider Threat no se mide solo por su capacidad preventiva, sino también por su aptitud para responder de forma ágil, proporcional y legalmente válida ante un incidente. Un plan de respuesta ante amenazas internas debe ser estandarizado, repetible y consistentemente aplicado, cubriendo todo el ciclo del incidente (CISA, 2020).

Un plan de respuesta debe incluir al menos los siguientes elementos (CISA, 2020):

- Ámbito de aplicación y tipología de incidentes cubiertos (robo de PI, sabotaje, filtración, error humano, etc.)

- Roles y responsabilidades del equipo de respuesta, con canales de comunicación definidos
- Procedimientos de activación, recolección de evidencias, investigación, documentación y cierre
- Escalado interno y criterios para involucrar a recursos externos si fuera necesario
- Normas de proporcionalidad, confidencialidad y respeto a derechos laborales

Por lo tanto, tal y como propone SIFMA (2024), la respuesta debe seguir una lógica estructura, mostrada en la Tabla 6.

FASE	OBJETIVO PRINCIPAL	ACCIONES CLAVE	RESPONSABLES EN CYNERDATA
1. DETECCIÓN Y CLASIFICACIÓN	Identificar la naturaleza y origen del incidente	Clasificación del incidente, activación de auditoría y UEBA/XDR	CISO
2. CONTENCIÓN Y MITIGACIÓN	Limitar el impacto inmediato y evitar propagación	Revocación de accesos, aislamiento de dispositivos o sistemas	CISO, responsable del programa
3. INVESTIGACIÓN INTERNA	Recopilar evidencias y analizar el incidente	Revisión de logs, entrevistas, documentación segura	RRHH, responsable del programa
4. DECISIÓN Y ACCIÓN	Determinar consecuencias disciplinarias, legales o correctivas	Evaluación de negligencia, medidas disciplinarias	Dirección, Compliance, RRHH, Asesoría jurídica
5. COMUNICACIÓN Y REPORTE	Informar internamente y cumplir con obligaciones externas	Informe al comité ejecutivo, notificación a autoridades (si procede), registro en sistema de incidentes	Responsable del programa, Dirección, Asesoría jurídica

TABLA 6

FASES DEL PLAN DE RESPUESTA ANTE INCIDENTES

Fuente: Elaborada a partir de SIFMA (2024)

6.1.7. EVALUACIÓN DEL PROGRAMA Y MEJORA CONTINUA

Por último, pero no por ello menos importante, entramos al apartado final de nuestro protocolo Insider Threat. Como ya sabemos, estos programas no consisten únicamente en contar incidentes. Se trata de construir una arquitectura sistemática que mida la eficacia real del protocolo en términos de prevención, detección, contención y aprendizaje organizacional. Por ello, la evaluación debe ser continua, dinámica y adaptada al momento de madurez del programa (INSA, 2022).

6.1.7.1. EVALUACIÓN SEGÚN LA ETAPA DE MADUREZ DEL PROGRAMA

Stewart & Handy (2024) proponen un modelo de madurez que permite a las organizaciones evaluar el grado de desarrollo, integración y efectividad de sus programas Insider Threat. Una empresa necesita estructuras claras para evaluar su capacidad de gestionar amenazas internas y comunicar su nivel de preparación a distintos públicos: desde la alta dirección hasta los reguladores externos.

Para estructurar la madurez, se aportan cinco distintos niveles (FFIEC, 2017 apud Stewart & Handy, 2024):

NIVEL	DESCRIPCIÓN
Baseline	Cumplimiento mínimo legal y regulatorio
Evolving	Procedimientos documentados, pero sin integración o automatización significativa
Intermediate	Procesos formalizados, con roles definidos y controles operativos
Advanced	Integración de la ciberseguridad en todas las áreas de negocio. Uso de análisis avanzados

Innovative	Liderazgo en innovación tecnológica y metodológica. Adopción temprana de soluciones emergentes

TABLA 7

NIVELES DE MADUREZ DEL PROGRAMA INSIDER THREAT

Fuente: Elaborada a partir de Stewart & Handy (2024)

Gracias a la Tabla 7, no se clasifica la organización en un único nivel. Esta permite asignar niveles diferentes a cada una de las categorías clave del programa Insider Threat. Estas categorías, las definen Stewart y Handy (2024) como:

1. Gestión de activos
2. *Backups*
3. Seguridad en la nube y en la red
4. Informes y reportes de usuario
5. Gestión, gobernanza y métricas
6. Gestión de identidad y acceso
7. Respuesta a incidentes
8. Monitorización
9. *Offboarding* y desvinculaciones
10. Gestión de riesgos
11. Inteligencia en las amenazas e intercambio de información
12. Formación, concienciación y EAP (Programas de Asistencia al Empleado, por sus siglas en inglés)
13. *Onboarding* e incorporaciones

Con estas categorías, la organización puede definir perfectamente el nivel en el que se encuentran con respecto a cada una de ellas. Por ejemplo, en *Gestión de activos*, la empresa puede estar en un nivel *Advanced*, pero en *Respuesta a incidentes*, estar aún en *Evolving*.

Gracias a esta clasificación, el equipo puede revisar cada categoría y asignar un estado (alto, medio, bajo) según su implementación real, como se muestra en la Imagen14,

creando una matriz que permite ver en qué nivel se encuentra cada categoría y dónde debe mejorarse.

Este modelo tiene múltiples beneficios además de poder realizar una autoevaluación estructurada: permite priorizar recursos, presentar de forma clara y visual el estado del programa, construir una hoja de ruta de mejora continua y adaptarse al riesgo en función de los recursos de la organización.

MAGEN 14

SIMULACIÓN DE HALLAZGOS DE LA EVALUACIÓN DEL MODELO DE MADUREZ

Fuente: Stewart y Handy (2024)

6.1.7.2. CINCO DIMENSIONES CLAVE PARA LA EFICACIA

Burgess (2024) evalúa estos programas según cinco grandes dimensiones estratégicas:

1. Riesgo: evaluar si el programa realmente reduce la exposición al riesgo aceptado por la organización
2. Comunicación: medir la comprensión del protocolo por parte de empleados y directivos
3. Educación: evaluar si las formaciones han cambiado comportamientos o actitudes

4. Armonización: verificar si el programa se alinea con normativas y estándares del sector
5. Alineación estratégica: comprobar si el protocolo contribuye a los objetivos globales de la organización

Si se requiere, la organización puede poner en marcha indicadores concretos como, por ejemplo: el porcentaje de personal que reconoce los indicadores de un insider, tiempo medio desde la detección hasta la contención, número de reportes voluntarios de comportamiento sospechoso, etc (Burgess, 2024).

6.1.7.3. HERRAMIENTAS DE EVALUACIÓN ESTRUCTURADA

Existen herramientas fundamentales para la evaluación y mejora de estos programas: el *Insider Threat Vulnerability Assessment* (ITVA) y el *Insider Threat Program Evaluation* (ITPE). Estas están diseñadas para proporcionar a las organizaciones una metodología para identificar vulnerabilidades y evaluar la eficacia de sus programas de gestión de amenazas internas (Black, 2024).

6.1.7.3.1. INSIDER THREAT VULNERABILITY ASSESSMENT (ITVA)

El ITVA es una herramienta que permite identificar y comprender las vulnerabilidades existentes que podrían ser explotadas por amenazas internas. Se centra en áreas como la cultura organizacional, la supervisión de empleados, la protección de datos y la gestión de accesos. Al utilizar ITVA, las organizaciones pueden:

- Evaluar la preparación de la organización para prevenir, detectar y responder a amenazas internas
- Identificar brechas en políticas, procedimientos y controles técnicos
- Priorizar áreas de mejora para fortalecer la postura de seguridad interna (Black, 2024)

6.1.7.3.2. INSIDER THREAT PROGRAM EVALUATION (ITPE)

El ITPE evalúa la madurez y eficacia de un programa Insider Threat existente. Se basa en prácticas recomendadas y estándares de la industria para proporcionar una evaluación objetiva del modelo. Esta permite:

- Medir el rendimiento del programa en áreas clave como la gobernanza, formación, supervisión y respuesta a incidentes.
- Identificar fortalezas y debilidades en la implementación del programa
- Desarrollar un plan de acción para mejorar continuamente el programa y adaptarlo a las amenazas emergentes.

NIVEL	ITVA	ITPE
1. NO REALIZADO	Existe una falla total en su capacidad para desempeñar esta función. No está preparada para prevenir, detectar ni responder al riesgo	No se cumple con las capacidades mínimas esperadas
2. CORE (BÁSICO)	Cuenta con controles mínimos. Puede detectar el riesgo, pero tiene dificultades para prevenirlo o responder de forma eficaz	Se ejecutan todas las prácticas mínimas establecidas
3. MEJORADO	Dispone de controles adecuados y puede detectar y responder a las amenazas internas, aunque todavía tiene dificultades en la prevención	Además de lo requerido, se han implementado prácticas adicionales para mejorar la eficiencia y funcionalidad
ROBUSTO	Existen controles y políticas excepcionales. La organización está plenamente preparada para prevenir, detectar y responder a amenazas internas	Cuenta con prácticas avanzadas y sostenidas para la gestión eficiente y continua del riesgo insider

TABLA 8

NIVELES DE EVALUACIÓN DEL ITVA Y DEL ITPE

Fuente: Elaborada a partir de Black (2024)

Como resumen de ambas herramientas, se presenta la Tabla 8 para entender un poco más como trabajan.

6.1.7.4. APLICACIÓN DE LA EVALUACIÓN Y MEJORA CONTINUA EN CYNERDATA SOLUTIONS S.L

Pongamos un ejemplo ficticio de la situación de nuestra empresa, para ver como quedaría reflejada la evaluación desde dentro:

Con base en los niveles de madurez, se ha revelado que Cynerdata Solutions se encuentra en un nivel intermedio-avanzado en categorías como la gestión de activos, gobernanza y formación y EAP. Sin embargo, en dimensiones como *offboarding* e inteligencia, la madurez se encuentra en el estado *evolving*, por lo que se han trazado líneas de acción para elevar estas categorías en el próximo ciclo anual de revisión.

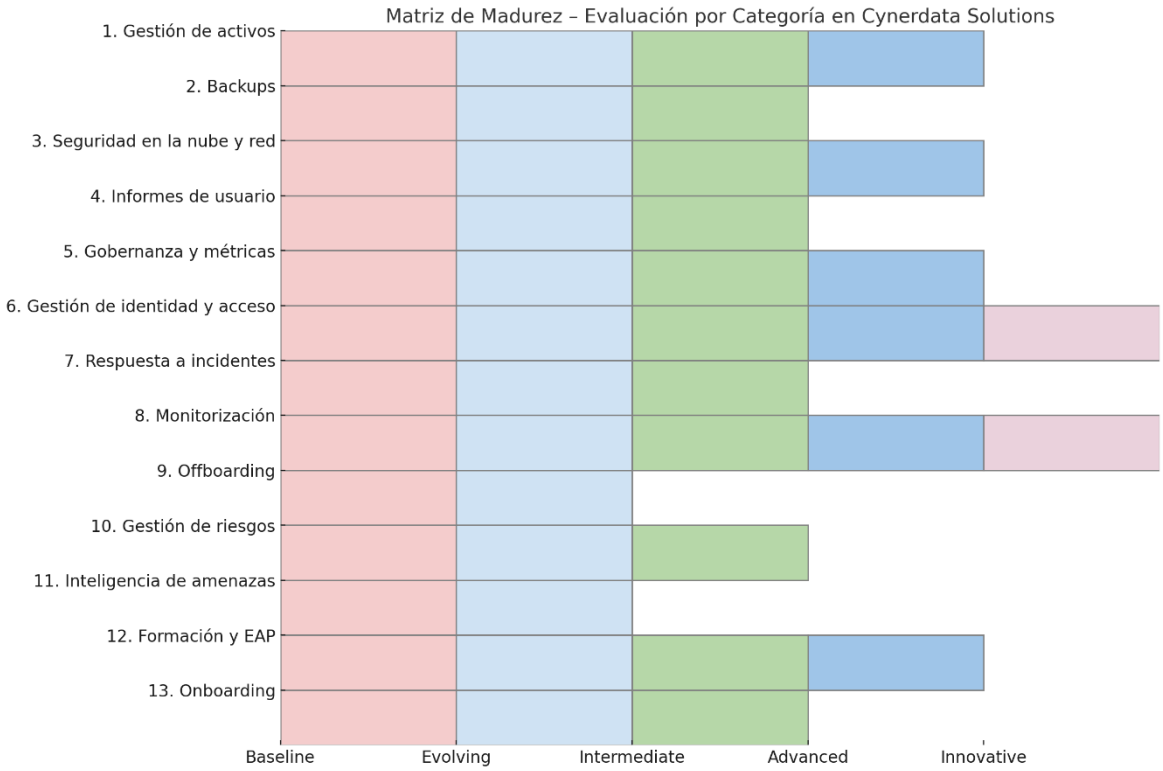


IMAGEN 15

MATRIZ DE MADUREZ DEL PROGRAMA INSIDER THREAT EN CYNERDATA SOLUTIONS

Fuente: Elaboración Propia

Para visualizar esta información, se ha creado una matriz como representación visual de los niveles alcanzados en la empresa, mostrados en la Imagen 15.

En cuanto a las cinco dimensiones de eficacia:

1. Riesgo: se han reducido en un 40% los accesos injustificados a activos críticos desde la implementación del sistema UEBA.
2. Comunicación: más del 85% de los empleados afirma comprender las normas internas de seguridad y saber a quién reportar un incidente.
3. Educación: la tasa de clics en simulaciones de phishing ha descendido del 18% al 6% en los últimos dos trimestres.
4. Armonización: el protocolo se ha alineado con todas las guías implementadas.
5. Alineación estratégica: se ha integrado en su totalidad en la estrategia global de ciberseguridad y sostenibilidad.

Finalmente, se comenzaron a usar de forma "piloto" las herramientas ITVA e ITPE:

- ITVA: permitió identificar como debilidades críticas la baja formalización del proceso de offboarding y la escasa trazabilidad de acceso a repositorios de documentación confidencial.
- ITPE: reveló una cobertura sólida en gobernanza, supervisión técnica y formación, pero oportunidades de mejora en el intercambio de inteligencia y la evaluación en procesos de selección.

En ambas herramientas, la mayoría de las áreas auditadas obtuvieron una puntuación entre nivel 2 (Core) y nivel 3 (Mejorado), con algunas emergentes acercándose a un nivel 4 (Robusto).

Se plantea un plan de mejora para este año en base a las evaluaciones realizadas:

- Formalizar e integrar el protocolo de offboarding con RRHH y Legal.
- Avanzar hacia un sistema de puntuación de riesgo individual
- Consolidar como estándar definitivo el ciclo IPDRR al completo

7. CONCLUSIONES

Las amenazas internas representan uno de los mayores desafíos contemporáneos en materia de ciberseguridad. A diferencia de los ataques externos, el insider cuenta con legitimidad de acceso, conocimiento profundo de los sistemas y, a menudo, con la confianza implícita de la organización. Esto hace que su detección y prevención requiera enfoques más sofisticados, proactivos y multidisciplinares.

Este Trabajo Fin de Grado ha demostrado que es posible diseñar un protocolo integral y escalable de prevención de amenazas internas adaptado al contexto de una empresa tecnológica con entorno híbrido. La integración de marcos como el ciclo IPDRR, herramientas de analítica de comportamiento como UEBA y buenas prácticas organizativas han permitido establecer una propuesta teórica coherente, fundamentada y alineada con los principales estándares internacionales.

Asimismo, se ha puesto de manifiesto que la prevención del insider threat no puede abordarse únicamente desde lo técnico: es imprescindible fomentar una cultura de seguridad sólida, transversal y compartida, así como establecer canales de comunicación efectivos, procesos de offboarding seguros y evaluaciones periódicas del riesgo interno.

Entre los principales aportes de este trabajo destacan:

- La identificación de factores humanos y organizativos que favorecen la aparición del insider.
- La propuesta de un protocolo adaptado a un caso práctico, Cynerdata Solutions, S.L., que sirve como modelo replicable.
- El uso combinado de herramientas conductuales, formativas y evaluativas (ITVA, ITPE, etc.) como pilares de una estrategia integral.

Por último, cabe señalar que, aunque el protocolo no ha sido implementado en un entorno real, su valor reside en ofrecer un marco estructurado para empresas que desean iniciar o mejorar su estrategia de prevención de amenazas internas. La protección del conocimiento, de las personas y de la reputación corporativa no es solo una cuestión técnica, sino estratégica.

8. BIBLIOGRAFÍA

AENOR (2022). *Information security, cybersecurity, and privacy protection — Information security management systems — Requirements ISO 27001:2022*. Madrid: Asociación Española de Normalización y Certificación.

Ali, A., Ahmed, M., Ilyas, M., & Küng, J. (2017). Mitis-an insider threats mitigation framework for information systems. In *Future Data and Security Engineering: 4th International Conference, FDSE 2017, Ho Chi Minh City, Vietnam, November 29–December 1, 2017, Proceedings 4* (407-415). Springer International Publishing.

Alsowail, R. A., & Al-Shehari, T. (2021). A multi-tiered framework for insider threat prevention. *Electronics*, *10*(9), 1005.

Arroyo Varela, S. (2020). *Fundamentos de inteligencia competitiva.* [Documento académico].

Auditool (2024). Principios Básicos de Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad (CIA). https://www.auditool.org/blog/auditoria-de-ti/principios-basicos-de-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad-cia

Barrutieta, L. H., & Ursúa, M. P. (2011). La psicopatía subclínica y la triada oscura de la personalidad. *Behavioral Psychology= Psicología Conductual*, *19*(2), 317.

Beucher, M. (2024). Principios de la seguridad de la información: ¿Cuáles son? En *CiberseguridadTips*. https://ciberseguridadtips.com/principios-seguridad-informacion/

Black, R. (2024). CERT Releases 2 Tools to Assess Insider Risk. Software Engineering Institute (SEI). Carnegie Mellon University. https://kilthub.cmu.edu/articles/online_resource/CERT_Releases_2_Tools_to_Assess_Insider_Risk/25321078?file=44757511

Burgess, C. (2023). 5 Key Areas to Help Measure your Insider Risk Program Effectiveness. DTEX Systems. https://www.dtexsystems.com/blog/measuring-the-efficacy-of-your-insider-risk-program/

Burke, B.M (2024). Windows Management and Cybersecurity: Latest Security Threats and Mitigation Strategies. *Old Dominion University. CYSE 280: Windows System Management and Security*

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)*. Addison-Wesley.

Cano, J. J. (2011). Amenazas persistentes avanzadas, inteligencia y contrainteligencia en un contexto digital. *Revista Sistemas*, *119*.

Cibersecurity Insiders (2023). *2023 Report. Insider Threat*.

Clifton, A. (2024). *Strategies for Insider Threat Mitigation and Detection* (Doctoral dissertation, Walden University).

Cybersecurity and Infrastructure Security Agency (CISA) (2020). *Insider threat mitigation guide*. U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide

Cybersecurity and Infrastructure Security Agency (CISA) (2024). *Principios básicos sobre amenazas de agentes internos: lo que necesita saber. FACT SHEET*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2024-09/insider-threat-101-fact-sheet_07-29-2024_508_ES.pdf

Confederation of European Security Services (CoESS) (2019). *Insider Threat Program Development - Management Manual*.

De Diego, J (2025). *Introducción a los productos de HashiCorp*. https://www.bluetab.net/es/introduccion-a-los-productos-de-hashicorp/

Díaz Caneja, J. M. (2021). Contrainteligencia en la protección de la actividad empresarial. En *Seguritecnia: Inteligencia en el ámbito de la seguridad corporativa*. https://www.seguritecnia.es/tecnologias-y-servicios/inteligencia/contrainteligencia-en-la-proteccion-de-la-actividad-empresarial_20210122.html

Eckstein, C. (2015). *Preventing data leakage: A risk based approach for controlled use of the use of administrative and access privileges*. Trabajo dirigido por Carbone, R. The SANS Institute, agosto.

FFIEC. (2017). Cybersecurity assessment tool. Federal Financial Institutions Examination Council (FFIEC). https://www.ffiec.gov/sites/default/files/media/resources/FFIEC_CAT_May_2017.pdf

Fortinet (2025). Tríada CIA: confidencialidad, integridad y disponibilidad. https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

Gelman, H., Hastings, J. D., Kenley, D., & Loiacono, E. (2024). Toward an Insider Threat Education Platform: A Theoretical Literature Review. *arXiv preprint arXiv:2412.13446*.

González, R. (2022). *#1 - Control de acceso a la información: principio del mínimo privilegio*. LinkedIn. https://www.linkedin.com/pulse/1-control-de-acceso-la-informaci%C3%B3n-principio-del-m%C3%ADnimo-gonzalez/

González Moraga, F. R. (2015). La tríada oscura de la personalidad: maquiavelismo, narcisismo y psicopatía. Una mirada evolutiva. *Criminalidad*, *57*(2), 253-265.

Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal*, 103068.

Intelligence and National Security Alliance (INSA) (2022). Measuring the Effectiveness of Insider Threat Programs. INSA. https://www.insaonline.org/docs/default-source/default-document-library/2022-white-papers/insa_wp_effectiveness.pdf

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A. M. (2015). Insider threat detection study. *NATO CCD COE, Tallinn*.

Lee, D., Lallie, H. S., & Michaelides, N. (2023). The impact of an employee's psychological contract breach on compliance with information security policies: intrinsic and extrinsic motivation. *Cognition, Technology & Work, 25(2), 273-289.*

López Grande, C. E. (2015). Ingeniería social: el ataque silencioso. *Revista Tecnológica: no. 8*.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mylrea, M., Gourisetti, S. N. G., Larimer, C., & Noonan, C. (2018). Insider threat cybersecurity framework webtool & methodology: Defending against complex cyber-physical threats. In *2018 IEEE Security and Privacy Workshops (SPW)* (207-216). IEEE.

Montoya, F. (2019). Inteligencia económica y contrainteligencia empresarial, herramientas necesarias para competir. En Interempresas*: Seguridad y Vigilancia*. https://www.interempresas.net/Seguridad/Articulos/260010-Inteligencia-economica-contrainteligencia-empresarial-herramientas-necesarias-competir.html

Mujinga, M., Eloff, M. M., & Kroeze, J. H. (2017). A socio-technical approach to information security. *ResearchGate*. https://www.researchgate.net/publication/320288245_A_socio-technical_approach_to_information_security

National Counterintelligence and Security Center (NCSC) (2024). *Insider Threat Guide. A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*.

National Counterintelligence and Security Center (NCSC) (2024). *Protect your Organization from the Inside Out. Government Best Practices*.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. *2014 IEEE security and privacy workshops* (214-228). IEEE.

Real Academia Española (RAE) (2024). *Contrainteligencia*. https://dle.rae.es/contrainteligencia?m=form

Real Academia Española (RAE) (2024). *Inteligencia*. https://dle.rae.es/inteligencia?m=form

Real Academia Española (RAE) (2024). *Seguridad*. https://dle.rae.es/seguridad?m=form

Ruohonen, J., & Saddiqa, M. (2024). What Do We Know About the Psychology of Insider Threats?. *https://arxiv.org/abs/2407.05943*

Salman, A. (2025). La Contra-Inteligencia y la Seguridad en el sector empresarial. En *Legítima Defensa*. https://www.legitimadefensa.com.ar/seguridad/seguridad-empresarial/la-contra-inteligencia-y-la-seguridad-en-el-sector-empresarial/

Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. New York, NY: John Wiley & Sons.

Schoenherr, J. R. (2022). Insider threats and individual differences: Intention and unintentional motivations. *IEEE Transactions on Technology and Society, 3(3), 175-184.*

Schoenherr, J. R., & Thomson, R. (2021). The cybersecurity (CSEC) questionnaire: Individual differences in unintentional insider threat behaviours. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (1-8). IEEE.

Schulze, H. (2024). New Report Reveals Insider Threat Trends, Challenges, and Solutions. En *Cibersecurity Insiders*.

Securities Industry and Financial Markets Association (SIFMA) (2024). *Insider threat best practices guide*. https://www.sifma.org/wp-content/uploads/2025/03/2024-SIFMA-Insider-Threat-Best-Practices-Guide-FINAL.pdf

Shaikh, A. & Oliveira, D. Informal IT and Routine Activity Theory -A Theoretical Review (2019). *2019 SoutheastCon, Huntsville, AL, USA, (1-4). IEEE*

Software Engineering Institute (SEI) (2022). Common Sense Guide to Mitigating Insider Threats, Seventh Edition. https://insights.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/.

Stewart, A., & Handy, M. (2024). The Design and Implementation of an Insider Threat Maturity Model. *Counter-Insider Threat Research and Practice*.

Toelle, E. (2021). *Microsoft 365 Compliance: A Practical Guide to Managing Risk* (289-314). Apress.

Vashisth, A., & Kumar, A. (2013). Corporate espionage: The insider threat. *Business information review*, *30*(2), 83-90.

Vilas Rodríguez, J. (2017). La contrainteligencia en el sector de la industria. *Economía industrial*, (405), 133-141.

Wang, Z. Q., & El Saddik, A. (2023). DTITD: an intelligent insider threat detection framework based on digital twin and self-attention based deep learning models. *IEEE Access*, *11*, 114013-114030.

Whitelaw, F., Riley, J., & Elmrabit, N. (2024). A review of the insider threat, a practitioner perspective within the uk financial services. *IEEE Access*, *12*, 34752-34768.