

UNIVERSIDAD
INTERNACIONAL
DE LA RIOJA



GESTIÓN DE LA SEGURIDAD Y ANÁLISIS DE RIESGOS

Actividad: Informe de análisis de riesgos

Descripción breve

Informe de resultados obtenidos en el análisis de riesgos

DANIEL BARBEYTO TORRES

DANIEL BARBEYTO TORRES

Contenido

1.	Introducción	2
2.	Desarrollo del análisis	3
3.	Plan de tratamiento.....	7

1. Introducción

Descripción breve de la compañía.

Industrias Vaine es una organización multinacional de tecnología con sede en **Gotan City**, la cual está especializada en el desarrollo e implementación de soluciones de ciberseguridad, inteligencia y comunicaciones seguras. Dicha organización gestiona activos de información muy críticos, lo que motiva la realización de un análisis de riesgos, y la necesidad estratégica de la dirección (entre ellos el propietario, Bruno Vaine) de formalizar su seguridad.

Aunque la empresa cuenta con controles técnicos robustos, tiene la intención de adaptarse progresivamente a una norma de gestión estándar, en concreto la ISO 27001, para poder garantizar la integridad del nuevo prototipo avanzado de inteligencia artificial y de defensa llamado “Proyecto Alfredo de Gotan”.

Descripción detallada del contexto.

Contexto Interno

El objetivo principal de la compañía es liderar la innovación tecnológica en defensa. No obstante, se ha detectado una cultura de seguridad que carece de formalización oficial (por ejemplo, falta de políticas y roles documentados o procedimientos informales de uso de la información).

La compañía cuenta con personal técnico y equipos de respuesta a incidentes altamente cualificados, pero sus capacidades están limitadas al uso de procedimientos informales. Es destacable la falta de una normativa sobre el uso y protección de la información crítica de la organización.

Las actividades principales se centran en el desarrollo e implementación de prototipos militares. A nivel de procesos operativos, la empresa cuenta con la última tecnología y mantenimiento para el desarrollo del producto, no obstante se ha detectado una ausencia total de planes de contingencia y procedimientos de recuperación formalizados.

Por último, cabe destacar que Industrias Vaine cuenta con una infraestructura lógica muy avanzada, incluyendo un CPD propio o un firewall perimetral interno, entre otros. Estos activos son los que sustentan al “Proyecto Alfredo de Gotan”, pero es requerida una revisión de los controles lógicos para ser normalizados y estandarizados, aumentando consecuentemente su eficacia.

Contexto Externo

La compañía realiza sus actividades en un entorno hostil como es Gotan City, con altas tasas de criminalidad y ciberataques constantes. Debido a la naturaleza defensiva de la empresa y la presión ejercida por los competidores, se realizan complejas normativas de protección de datos.

Además, debido a la dependencia de proveedores críticos para la organización y el riesgo de incidentes ambientales por el entorno externo de la empresa, es condicionada la disponibilidad del “Proyecto Alfredo de Gotan”.

Riesgo asumible

Debido a la naturaleza de la organización, está dispuesta a asumir un riesgo bajo, idealmente residual. Esto se debe a su especialidad en soluciones de ciberseguridad, inteligencia y comunicaciones seguras. Las amenazas y ataques sobre activos críticos de la empresa supondrían tanto un impacto económico drástico, como un impacto reputacional por la exigencia de los clientes. Es por ello por lo que ningún riesgo que no sea bajo podrá ser tolerado sin un plan de tratamiento obligatorio.

Alcance

Como hemos mencionado, el análisis de riesgos abarcará los activos críticos, procedimientos, personal, ubicaciones y departamentos involucrados en todo el ciclo de vida del “Proyecto Alfredo de Gotan”.

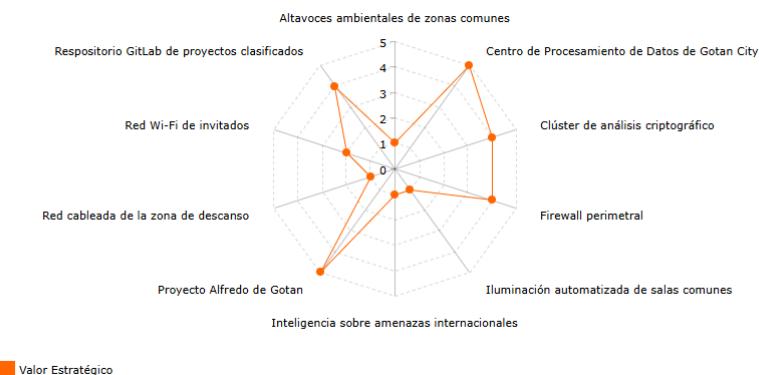
Limitaciones

El análisis de riesgos realizado se centrará en la evaluación del nivel de madurez de los controles actualmente implementados en la organización (basado en la preauditoría inicial). Son excluidos de esta iteración del análisis de riesgos los dominios de control no mencionados, siendo tratados en fases posteriores del sistema de gestión de la seguridad de la información.

2. Desarrollo del análisis

Identificación y valoración de activos

Para la realización del análisis de riesgos se del “Proyecto Alfredo de Gotan”, se han identificado 10 activos críticos de Industrias Vaine. Se ha usado una escala de valoración del 1 (Muy Bajo) al 5 (Muy alto) para indicar la criticidad del activo para la continuidad y confidencialidad del negocio.



La mayoría de los activos han recibido una valoración mayor al 4 (Alta) debido a la naturaleza sensible del Proyecto Alfredo de Gotan. A continuación se muestran los más críticos:

- **Centro de Procesamiento de Datos de Gotan City:** Instalación física donde se concentran los servidores y almacenamientos que soportan los sistemas críticos de la organización.
- **Proyecto Alfredo de Gotan:** Activo principal del análisis de riesgo. Prototipo avanzado que combina tecnología de inteligencia artificial y capacidades defensivas de última generación.
- **Repositorio Gitlab de proyectos clasificados:** Plataforma de control de versiones que almacena el código fuente de los proyectos de defensa, inteligencia y comunicaciones seguras.
- **Clúster de análisis criptográfico:** Conjunto de servidores dedicado a pruebas de algoritmos criptográficos y análisis de comunicaciones cifradas.
- **Firewall perimetral:** Dispositivo de seguridad perimetral que filtra el tráfico entre Internet y la red interna, mitigando ataques externos.

El resto de los activos no mencionados actúan como soporte para la actividad de la compañía.

Análisis de las amenazas

Una vez identificadas las amenazas según el catálogo MAGERIT mediante eMarisma, se han seleccionado las 5 amenazas más significativas para la compañía y realizado un análisis de los resultados obtenidos para justificar la necesidad inmediata de un aumento del nivel de madurez de la gestión de riesgos.

Amenaza 1: Divulgación de información sobre el CPD de Gotan City

Código: [A.19]

Probabilidad de ocurrencia: 100%

Riesgo estimado: 500

Riesgo resultante: 268.201

Métodos de ataque:

- + Manipulación del personal descontento para obtener credenciales.
- + Filtración de datos por el personal debido a la falta de una normativa de seguridad.
- + Escucha de comunicaciones no cifradas sobre la ubicación del CPD.

Impacto potencial:

- + Exposición de la infraestructura física a ataques directos por filtración de información.
- + Pérdida de la ventaja competitiva.
- + Pérdida de confianza de inversores.
- + Graves sanciones por el incumplimiento de una normativa de seguridad.

Medidas de mitigación:

- + NDA (Acuerdos de confidencialidad): Implementación de contratos estrictos para asegurar la confidencialidad por toda la plantilla.
- + Uso de herramientas que monitoricen la salida de información sensible.

Conclusión: Debe formalizarse de inmediato una política de seguridad para reducir las vulnerabilidades provocadas por el factor humano.

Amenaza 2: Divulgación de información sobre el Proyecto Alfredo de Gotan

Código de amenaza: [A.19] Divulgación de información

Probabilidad de ocurrencia: 100%

Riesgo estimado: 500

Riesgo resultante: 268.201

Métodos de ataque:

- + Manipulación del personal descontento para obtener credenciales.
- + Filtración de datos por el personal debido a la falta de una normativa de seguridad.
- + Transferencia y captura de archivos no cifrados con información del proyecto.

Impacto potencial:

- + Plagio del proyecto y pérdida de la ventaja competitiva.
- + Pérdida de la inversión en I+D realizada.
- + Graves sanciones por el incumplimiento de una normativa de seguridad.

Medidas de mitigación:

- + Cifrado seguro de todos los documentos y comunicaciones relacionadas con el proyecto
- + Uso de herramientas de monitorización sobre la salida de información sensible.

Conclusión: El riesgo es crítico dado que el activo sobre el que recae esta amenaza es el principal del negocio. La falta de normalización y eficiencia de los controles aplicados exponen a la empresa a múltiples vulnerabilidades.

Amenaza 3: Divulgación de información sobre el repositorio GitLab de proyectos clasificados

Código de amenaza: [A.19]

Probabilidad de ocurrencia: 100%

Riesgo estimado: 400

Riesgo resultante: 214.561

Métodos de ataque:

- + Manipulación del personal descontento para obtener credenciales.
- + Filtración de datos por el personal debido a la falta de una normativa de seguridad.
- + Exposición accidental del repositorio por error humano.

Impacto potencial:

- + Exposición del código fuente y pérdida de la ventaja competitiva
- + Daño reputacional grave ante clientes de la organización.

Medidas de mitigación:

+ Obligación de uso de sistemas de autenticación para todos los accesos al repositorio.

+ Auditorías periódicas de los roles y permisos establecidos.

Conclusión: Se deben tomar acciones urgentes para asegurar el ciclo de vida del I+D.

Amenaza 4: Errores del administrador sobre el Proyecto Alfredo de Gotan

Código de amenaza: [E.2]

Probabilidad de ocurrencia: 80%

Riesgo estimado: 320

Riesgo resultante: 163.832

Causas del Error:

- + Actualizaciones que causan caídas por no ser revisadas en un entorno de laboratorio previo.
- + Asignación accidental de permisos a empleados que no deberían tener dichos privilegios.

Impacto potencial:

- + Borrado involuntario de ficheros por falta de conocimiento del rol.
- + Paradas parciales o totales del desarrollo del “Proyecto Alfredo de Gotan” por fallos del sistema.
- + Aparición de vulnerabilidades o desactivación de controles o defensas.

Medidas de mitigación:

+ Implementación y formalización de políticas de gestión de cambios.

+ Implementación y formalización de una política de backups y snapshots para la recuperación del sistema en caso de error.

Conclusión: Sin guías de administración formalizadas, el administrador puede confundirse y provocar fallos y caídas en el sistema.

Amenaza 5: Acceso no autorizado sobre el CPD de Gotan City

Código de amenaza: [A.11]

Probabilidad de ocurrencia: 80%

Riesgo estimado: 320

Riesgo resultante: 172.296

Métodos de ataque:

- + Uso de credenciales sustraídas para superar el perímetro de seguridad.
- + Movimiento lateral del atacante al CPD infectando uno de los equipos de la organización.

Impacto potencial:

- + Sabotaje al hardware o software de la empresa, provocando daños directos.
- + Robo de información y activos con información clasificada.

Medidas de mitigación:

- + Implementación de una segmentación de red que aisle lógicamente la red de gestión del CPD del resto de la organización.
- + Implementación de un control de acceso físico avanzado para la protección de activos físicos.

Conclusión: El 80% de probabilidad de ocurrencia de un acceso no autorizado al CPD refleja la necesidad de endurecer su defensa y controles mediante una estrategia formalizada.

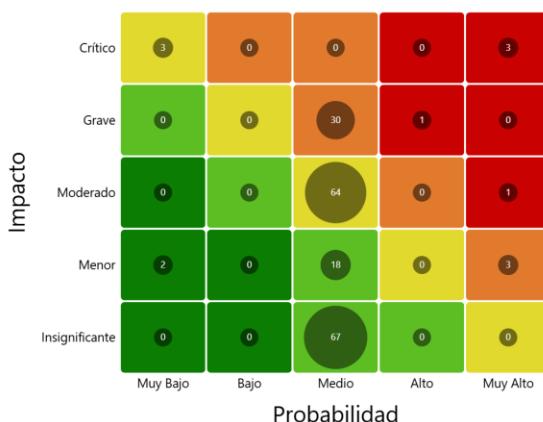
Resultados gráficos

En la siguiente Figura podemos ver dos Mapas de calor que representan la evolución del perfil del riesgo tras el análisis de riesgos.

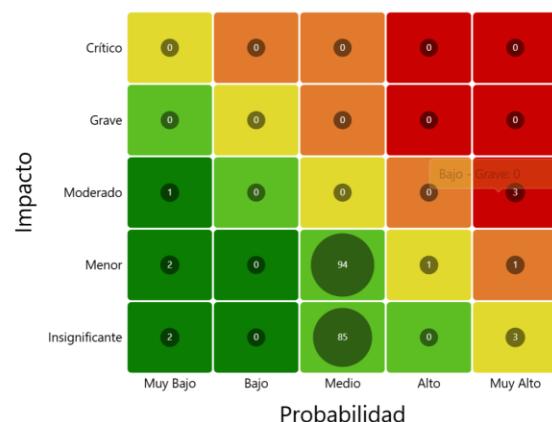
El Mapa de Riesgo Estimado (Izquierda) tiene una significativa presencia en los cuadrantes Grave y Moderado, indicando que una gran parte de los riesgos tendrían un gran impacto en la organización. Estos riesgos corresponden, entre otros, a faltas de controles sobre el Proyecto Alfredo de Gotan o sobre el CPD de Gotan City.

Por otro lado, el Mapa de Riesgo Resultante (Derecha) evidencia un desplazamiento vertical de los riesgos hacia las zonas de impacto Menor o Insignificante, pero sin un mejorías notables en la probabilidad de ocurrencia.

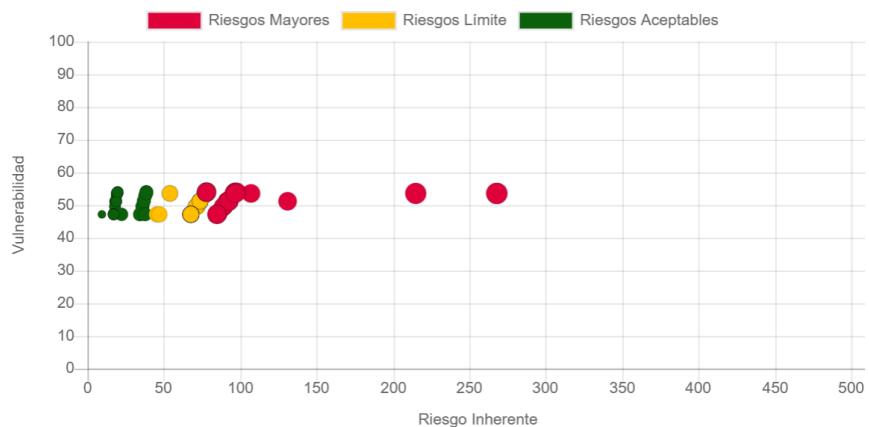
Riesgo Puro



Riesgo Residual



A continuación, la siguiente Figura muestra el nivel de exposición del sistema (Vulnerabilidad) comparado con el valor de Riesgo Resultante (“Riesgo Inherente”). Aunque la mayoría de riesgos se ubican en la zona de “Riesgos Aceptables”, podemos ver un porcentaje significativo de ellos en los niveles de “Riesgos Mayores” y “Riesgos Límite”. Además en ella destacan unos valores atípicos en rojo (en torno a 200 y 300 de Riesgo Inherente) que corresponde a las amenazas al CPD y al Proyecto Alfredo de Gotan analizadas en la sección anterior.



3. Plan de tratamiento

Plan de tratamiento 1: Proceso Disciplinario

Código general: [A.06.04]

Responsable: Departamento de RRHH y Responsable de SI

Riesgo Residual Final: Bajo / Aceptable

Nombre Control: Proceso Disciplinario

Fecha Prevista: 1/3/26 Fecha Fin Previsión: 1/5/26 Fecha Ejecución: 1/6/26

Plan: Definición, formalización y comunicación de políticas sancionadoras vinculadas a la política general de seguridad de la información de la organización. Se incluirán cláusulas específicas en los contratos laborales que nombren los procedimientos disciplinarios relacionados con el incumplimiento de diferentes responsabilidades o obligaciones.

Resultado: Disuasión de comportamientos malintencionados por parte de la plantilla aplicando de forma estandarizada sanciones o despidos procedentes en caso de incidentes de seguridad intencionados.

Plan de tratamiento 2: Aprendizaje de los incidentes de seguridad de la información

Código general: [A.05.27]

Responsable: Responsable de SI y Equipo de Respuesta a Incidentes

Riesgo Residual Final: Bajo / Aceptable

Nombre Control: Aprendizaje de los incidentes de seguridad de la información

Fecha Prevista: 1/4/26 Fecha Fin Previsión: 15/6/26 Fecha Ejecución: 1/7/26

Plan: Desarrollo y estandarización de un protocolo formal de análisis post-incidente para identificar las causas de los eventos y aprender de ellos. La inteligencia adquirida se usará para actualizar las políticas de seguridad y formación, así como el sistema de gestión de riesgos.

Resultado: Mejora continua de la defensa en la compañía. Los análisis se convierten en conocimiento que permite proteger a los activos ante posibles futuras amenazas similares.