

Documentación sobre el uso de IA – Actividad 1

Para enriquecer el análisis presentado en la **Actividad 1** titulada **Informe Reflexivo Técnico-Ético: Seguridad Defensiva y Rol del SOC**, me he apoyado de diversos recursos, entre estos una herramienta de IA generativa (*ChatGPT*). Se planteó una serie de *prompts* o instrucciones que le fueron proporcionadas para la generación de la información, para después reflexionar acerca de tal información en relación con el objetivo de la actividad. Del mismo modo, a través de la documentación de estas instrucciones se comprobará la efectividad en sus respuestas y su precisión con el tema solicitado.

Identificar los principios de la triada CIA en el caso

Primero se le proporcionó el caso con el objetivo de que la herramienta pudiera de antemano saber el contexto sobre el cual se desarrollan las solicitudes siguientes. En este mismo *prompt* se incluyeron las preguntas clave que se querían responder con respecto a la privacidad, integridad y disponibilidad de los datos en el contexto de la seguridad de la información, proporcionándole también una perspectiva encaminada sobre el tema.

“Analiza este pequeño caso, desde un enfoque relacionado a la seguridad defensiva:

Una organización detecta accesos indebidos a una cuenta administrativa. El sistema no se encuentra caído, pero se sospecha que la contraseña fue compartida entre empleados sin autorización formal.

Ahora, podrías decirme, considerando principios CIA (Confidentiality, Integrity, Availability), ¿cuál de estos podría verse más comprometido o afectado y darme tus razones? Rápidamente, podría afirmar que lo más afectado es la confidencialidad, dada la sospecha de haber compartido una contraseña sin autorización, ¿cierto? Igualmente quisiera tu análisis para los demás principios.”

A partir de esta instrucción se esperaba darle a la herramienta una idea incompleta, con la cual se esperaba obtener tanto una comprobación como una respuesta similar con respecto a los demás puntos solicitados, en este caso acerca de los

principios restantes que no fueron ejemplificados en el *prompt*. La respuesta obtenida fue favorable:

1. Confidentiality (Confidencialidad) → la más comprometida

Aquí coincido contigo al 100%.

Por qué:

- Una cuenta administrativa da acceso a información sensible del sistema.
- El compartir una contraseña sin autorización rompe directamente el principio de "acceso sólo para quien debe tenerlo".
- Aunque no haya evidencia de robo de datos, el simple acceso indebido ya es una violación de confidencialidad.

Conclusión:

Sí, es correcto afirmar que la confidencialidad es el principio más afectado, porque se pierde el control sobre quién puede ver información crítica.

2. Integrity (Integridad) → potencialmente comprometida

Aunque no se menciona que haya cambios maliciosos, aquí entra el riesgo, no sólo el daño confirmado.

Por qué podría verse afectada:

- Un usuario con privilegios administrativos puede:
 - Modificar configuraciones
 - Alterar registros
 - Crear o borrar cuentas
- Si la contraseña fue compartida, ya no es posible tribuir acciones a una persona específica (no hay trazabilidad).

Realmente la respuesta fue útil, aunque en cierto modo está limitada a resaltar solamente algunos elementos clave y las razones sobre cómo se ve vulnerado cada principio dentro del caso planteado. Considerando el contenido del *prompt*, la respuesta por parte de la IA fue acorde a lo solicitado, de lo cual se intuye que se requiere un poco más de especificación y/o detalle. No obstante, se considera que el contenido sirvió como una base para comenzar el análisis, además de dar una idea sobre lo más relevante para ser indagado; aunque la parte referente al análisis de estos principios CIA se basó mayormente en intuición y razonamiento personal, se hizo también el uso de fuentes informativas que reforzaran la crítica personal.

Identificar una relación con aspectos sociales y éticos

Lo que se solicitó a continuación consiste en relacionar el análisis anterior (sobre los principios CIA) con otros aspectos más que nada éticos y de conducta social,

identificando tanto las buenas prácticas como los límites sobre los cuales un profesional en la materia puede y debe actuar.

“Ahora, ¿cómo crees que lo que llevamos analizado se relaciona con los siguientes aspectos a considerar?

Cultura organizacional y concientización: Describe fallas de cultura o de concientización presentes en el caso.

Ética profesional: Explica los límites éticos que debe respetar un analista SOC ante esta situación.

Alcance autorizado: Justifica por qué un analista SOC no debe actuar fuera del alcance autorizado.”

Claramente, el *prompt* utilizado para esta ocasión fue un poco genérico en cuestión de contenido, que si bien incluye los aspectos lo que se pretende relacionar y explicación breve sobre lo que se busca, tiene muchos aspectos de mejora para obtener una respuesta mucho mejor, por ejemplo: proporcionar una perspectiva encaminada hacia una idea personal como se aplicó anteriormente.

1. Cultura organizacional y concientización

El incidente refleja fallas claras de cultura de seguridad, no sólo un error técnico.

Fallas evidentes:

- **Normalización del compartir contraseñas**
Esto indica que los empleados:
 - No comprenden la criticidad de una cuenta administrativa, o
 - La comprenden, pero la cultura no penaliza ni desalienta estas prácticas.

- **Ausencia de responsabilidad individual**

Al compartir credenciales:

- Se diluye la rendición de cuentas
- Se rompe el principio de “una identidad = una persona”

- **Probable falta de concientización formal**

Posiblemente no existen (o no se refuerzan):

- Programas de awareness
- Políticas claras y comunicadas sobre gestión de accesos

Relación con CIA:

Esta mala cultura es la raíz de la afectación a la **confidencialidad** y al riesgo sobre la **integridad**.

2. Ética profesional del analista SOC

Aquí es clave separar investigar de excederse.

Límites éticos que debe respetar:

- **No asumir culpables**

Aunque existan indicios, el analista:

- Analiza eventos y evidencias
- No emite juicios personales

- **Respeto a la privacidad**

El acceso a:

- Logs
- Sesiones
- Actividades de usuarios

debe limitarse exclusivamente al objetivo de la investigación.

- **Objetividad y trazabilidad**

El analista debe:

- Documentar hallazgos
- Evitar modificar evidencia
- Mantener la cadena de custodia si aplica

Ejemplo ético claro:

Un analista SOC **no debe** revisar correos personales o archivos privados "por si acaso", aunque tenga privilegios técnicos.



3. Alcance autorizado

Este punto conecta directamente con ética y control interno.

Por qué no debe actuar fuera del alcance:

- **Principio de mínimo privilegio**

Incluso en incidentes, el analista:

- Sólo actúa dentro de las funciones asignadas

- **Riesgo legal y organizacional**

Actuar fuera del alcance puede:

- Invalidar la investigación
- Generar problemas legales para la empresa

- **Preservación de la evidencia**

Acciones no autorizadas pueden:

- Alterar logs
- Contaminar pruebas
- Dificultar auditorías posteriores

Ejemplo práctico:

Si el alcance es *monitoreo y reporte*, el analista **no debe**:

- Cambiar contraseñas
- Bloquear cuentas
- Acceder directamente a sistemas productivos sin autorización explícita.



Se listaron de forma clara los puntos relevantes de cada aspecto solicitado, a lo cual mediante fuentes y sobre todo mediante el pensamiento crítico personal se complementó más a fondo todo lo identificado.

Explicación de términos ISC² y CBK

Como uso final, se solicitó algo simple en relación con dos conceptos importantes y con los cuales se reflexionó su intervención en un caso similar al que se analizó en la actividad.

“¿Podrías explicarme en qué consisten ISC² y CBK?”

A partir de esta instrucción, obtuvimos información concisa y breve para la reflexión tanto de las prácticas consideradas como adecuadas como de las normas sugeridas por consorcios especializados como lo es ISC², además de considerar la importancia de estos para garantizar la seguridad de la información.

¿Qué es ISC²?

ISC² (International Information System Security Certification Consortium) es una organización internacional sin fines de lucro dedicada a:

- Desarrollar estándares profesionales en ciberseguridad
- Emitir certificaciones reconocidas a nivel mundial
- Promover la ética profesional y las buenas prácticas en seguridad de la información

Es especialmente conocida porque certifica a profesionales que demuestran conocimientos técnicos, experiencia y conducta ética.

Certificaciones más conocidas de ISC²

- **CISSP** → Para profesionales senior en seguridad
- **SSCP** → Para roles operativos (SOC, analistas, administradores)
- **CC** → Nivel inicial (entry-level)
- **CSSLP, CCSP**, entre otras

👉 Algo clave:

Todas las certificaciones de ISC² requieren adherirse a un Código de Ética, no sólo pasar un examen.

¿Qué es el CBK (Common Body of Knowledge)?

El CBK es el cuerpo de conocimientos oficial definido por ISC².

En palabras simples:

El CBK es el **marco teórico y práctico** que establece **qué debe saber un profesional de ciberseguridad**.

No es un libro único, sino un **conjunto estructurado de dominios**, conceptos, principios y buenas prácticas.

Relación entre ISC² y CBK

- ISC² → la organización
- CBK → el contenido y conocimiento que la organización define y evalúa

Cada certificación de ISC² se basa en su propio CBK, organizado en dominios.

Por ejemplo:

- El CISSP CBK tiene 8 dominios
- El SSCP CBK tiene 7 dominios
- El CC CBK tiene 5 dominios

Ejemplo práctico (muy conectado con tu caso)

En el CBK se incluyen temas como:

- Control de acceso
- Gestión de identidades
- Principios CIA
- Ética profesional



Ante la respuesta obtenida, se consideró que para reflexionar al respecto no fue necesario extender más allá la investigación, pero para validarla se buscó más información al respecto (entre ella hubo alguna fuente académica), ya no solo para la validez de la información, sino para la comprensión adecuada del propósito y definiciones.

Si bien el uso de herramientas de IA generativa hoy en día resulta útil para simplificar conceptos clave e ideas relevantes, lo cierto es que el usuario es quien limita a través de su capacidad para redactar una instrucción lo suficientemente detallada que pueda ser interpretada por la IA para proporcionarle lo que busca. Esto se ha visto reflejado durante la documentación de su uso en esta actividad, incluso se aplicó el uso de instrucciones variadas en cuestión de especificación, y como se pudo observar, esta habilidad es clave al momento de usar este tipo de herramientas. Asimismo, el deber de quien las utiliza para el fin que sea es validar la información a través de fuentes confiables y certificadas, con lo que verifica la

veracidad y la precisión en la información generada, y además es importante no depender completamente de estas herramientas.