Dilemas éticos en ciberseguridad

Seguridad Informática II

Integrantes del Equipo:

López López Josué Emmanuel 182078

Mata Martínez Aaron Efraim 179419

Rodríguez Hernández Edgar Omar 177888

Rodriguez Morin Estefano Alessandro 178584

Ros Padilla Iván 177573

Salinas Carrillo Mauricio Josafat 177406

Profesor: Servando López Contreras

15 de marzo de 2026

Introducción

En el entorno actual, la ciberseguridad va más allá del dominio técnico; requiere un marco ético y legal sólido que guíe la toma de decisiones. Los profesionales de la información se enfrentan constantemente a dilemas complejos donde la protección de los activos, el cumplimiento de la ley y el respeto a la privacidad entran en conflicto, exigiendo un criterio profesional íntegro y normativo.

Esta actividad presenta el análisis estructurado de tres escenarios críticos: el acceso interno no autorizado, el hallazgo de vulnerabilidades financieras no reportadas y los límites éticos en el uso de herramientas OSINT. Cada caso es evaluado bajo enfoques éticos fundamentales y los mandamientos de la informática, justificando la postura técnica idónea para garantizar la responsabilidad social y corporativa.

Escenario 1: Acceso no autorizado interno

Trabajas en el área de ciberseguridad de una empresa. Durante una revisión de logs, detectas que un compañero accedió a correos privados del director general sin autorización. El compañero argumenta que lo hizo para “detectar posibles fugas de información”.

Identificación del dilema

El conflicto ético radica en la contraposición entre el deber percibido de protección (monitorear y prevenir fugas de información) y el respeto a la confidencialidad y privacidad de los altos mandos. Se cuestiona si un fin legítimo justifica el uso de medios ilícitos y unilaterales (romper el principio de privilegios mínimos y acceso autorizado) sin una orden explícita o un proceso formal de auditoría.

Aplicación de marcos éticos

- **A) Ética utilitarista:** El beneficio individual de "intentar descubrir una fuga" no supera el daño colectivo. Permitir accesos arbitrarios destruye la confianza institucional, desestabiliza el ambiente laboral y vulnera la estructura de gobernanza de la empresa, generando un perjuicio mayor para la organización.

- **B) Enfoque de derechos:** El director general posee el derecho fundamental a la privacidad de sus comunicaciones corporativas y personales. Este derecho solo puede ser suspendido bajo una investigación oficial autorizada por el

comité de ética o el área legal, por lo que el compañero violó flagrantemente este derecho.

- **C) Enfoque del bien común:** La seguridad de la información se sostiene sobre el respeto estricto a las políticas internas (como la Política de Uso Aceptable). Si cada analista actúa según su propio criterio, se disuelve el orden operativo y legal de la comunidad corporativa.

Relación con mandamientos

Violados:

- *Mandamiento 3:* "No indagarás en los archivos informáticos ajenos." (El colaborador husmeó en correspondencia privada sin un ticket o mandato de investigación).

- *Mandamiento 10:* "Utilizarás las computadoras respetando y considerando a tus semejantes." (Se ignoró el respeto profesional y la jerarquía organizacional).

Clasificación de delito

Delito informático: Se configura un acceso ilícito a sistemas, equipos o programas de informática (vulneración de la confidencialidad de los datos mediante el abuso de credenciales o funciones de administración).

Justificación profesional

Argumento técnico-ético: Como especialista en ciberseguridad, la prioridad es salvaguardar la Tríada CIA (Confidencialidad, Integridad y Disponibilidad), lo cual incluye el cumplimiento normativo interno. Ante el hallazgo en los logs, la acción técnica correcta es congelar y preservar la evidencia (bitácoras) para asegurar la cadena de custodia, y proceder al reporte inmediato ante el Comité de Ética, Recursos Humanos o la Dirección Jurídica. No se debe confrontar al compañero ni borrar la evidencia, sino seguir el Plan de Respuesta a Incidentes Internos para deslindar responsabilidades legales de manera institucional.

Escenario 2: Vulnerabilidad crítica no reportada

Durante un pentest encuentras una vulnerabilidad crítica en un sistema financiero que permite extraer dinero. El cliente aún no ha firmado el contrato final y tú sabes que podrías explotarla sin ser detectado.

Identificación del dilema

El dilema se presenta entre el beneficio económico y personal inmediato (lucro cesante mediante la explotación invisible de un fallo para extraer dinero) frente a la integridad profesional y la responsabilidad civil/penal de reportar una vulnerabilidad para proteger los activos financieros de terceros y la reputación del auditor.

Aplicación de marcos éticos

- **A) Ética utilitarista:** La explotación del fallo causaría pérdidas financieras masivas a los usuarios de la entidad y la quiebra reputacional de la empresa auditora. Reportarlo, en cambio, previene un impacto socioeconómico devastador, maximizando el bienestar de miles de cuentahabientes.
- **B) Enfoque de derechos:** Los usuarios del sistema financiero tienen derecho a la protección de su patrimonio y a la seguridad digital. Explotar la vulnerabilidad es una violación directa a sus derechos de propiedad y seguridad.
- **C) Enfoque del bien común:** El sistema financiero se basa en la confianza colectiva. Mantener la solidez y la seguridad de estas plataformas asegura la estabilidad económica de la sociedad, un bien común que el especialista debe defender.

Relación con mandamientos

- **Respetados (al reportarla):**
  - *Mandamiento 1:* "No usarás una computadora para dañar a otras personas."
  - *Mandamiento 4:* "No usarás una computadora para robar."
  - *Mandamiento 9:* "Pensarás en las consecuencias sociales del programa que escribas o del sistema que diseñes."

Clasificación del delito

- **Delito asistido por computadora:** El objetivo final de la acción maliciosa es el fraude financiero y el robo de activos (delitos patrimoniales tradicionales), utilizando el sistema informático y la explotación técnica como el medio ejecutor.

Justificación profesional

Argumento técnico-ético: En la práctica del *Pentesting*, la ausencia de un contrato final firmado no exime al profesional de los acuerdos de confidencialidad previos (NDA) ni del principio de buena fe contractual. La conducta técnica correcta exige detener cualquier interacción con el exploit, realizar una documentación detallada y formal del hallazgo en el reporte técnico y notificar de manera urgente a los canales de contacto oficiales del cliente bajo el marco de una *Divulgación Responsable (Responsible Disclosure)*. Explotar el fallo destruiría la carrera del auditor, violaría el código de ética de certificaciones internacionales (como CEH o CISSP) y derivaría en graves consecuencias penales.

Escenario 3: Uso de herramienta OSINT

Estás investigando a una persona sospechosa de fraude. Encuentras información personal (dirección, familia, hábitos) en fuentes abiertas. Tu superior te pide usar esa información para presionarlo psicológicamente.

Identificación del dilema

El conflicto se sitúa entre el cumplimiento de la obediencia jerárquica (acatar las órdenes de un superior para resolver un caso de fraude corporativo) y el cumplimiento de la legalidad y los límites éticos de la investigación (negarse a cometer acoso, extorsión o manipulación psicológica utilizando datos personales expuestos).

Aplicación de marcos éticos

- **A) Ética utilitarista:** Utilizar tácticas de coacción psicológica contamina el proceso legal. Si el sospechoso alega acoso u obtención ilícita de ventajas, las pruebas legítimas recopiladas podrían ser desestimadas en un juicio (teoría

del fruto del árbol envenenado), permitiendo que el defraudador quede libre. Actuar bajo la ley produce el mejor resultado para la empresa.

- **B) Enfoque de derechos:** Incluso un sospechoso de delito conserva sus derechos fundamentales al debido proceso, la dignidad humana y la protección de sus datos personales frente a actos de extorsión o intimidación. El investigador no posee facultades punitivas ni judiciales.
- **C) Enfoque del bien común:** La justicia debe operar bajo reglas claras y éticas. Permitir que los departamentos de seguridad corporativa actúen como "justicieros" al margen de la ley degrada el estado de derecho y deslegitima la profesión de la ciberseguridad.

Relación con mandamientos

- **Violados (al ejecutar la orden del superior):**
  - *Mandamiento 1:* "No usarás una computadora para dañar a otras personas." (Utilizar datos obtenidos digitalmente para infligir daño o presión psicológica).
  - *Mandamiento 10:* "Utilizarás las computadoras respetando y considerando a tus semejantes."

Clasificación del delito

- **Delito asistido por computadora:** Se utilizan herramientas tecnológicas de recolección de información (OSINT) y plataformas digitales como el medio principal para perpetrar un delito de extorsión, amenazas o acoso.

Justificación profesional

Argumento técnico-ético: Las metodologías de OSINT (Open Source Intelligence) tienen como límite la legalidad y el alcance técnico del objetivo. La información pública no equivale a información utilizable para fines delictivos como el hostigamiento o el *doxxing*. La postura profesional debe ser una negativa asertiva ante la orden de presión psicológica, procediendo a entregar únicamente un reporte técnico formal con las evidencias objetivas del fraude para que sea el equipo legal de la empresa quien actúe ante las autoridades correspondientes. Si el superior insiste, la situación debe ser escalada inmediatamente a la Dirección de Recursos Humanos o al canal de denuncias interno de la organización (*Whistleblowing*).