UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Universidad Politecnica de San Luis Potosi

Ingenieria en Tecnologias de la Informacion

Actividad 16

Dilemas eticos en ciberseguridad

Integrantes:

Coronado Noriega Jesus Olaf	178991
De La Rosa Rodriguez Erik	177700
Gonzalez Reyes Felipe de Jesus	181134
Mendoza Aguado Karina	179859
Serrano Zermeno Leonardo	177301
Perez Ventura Juan Alejandro	180370

Materia:
CNO V: Seguridad Informatica

Docente:
Servando Lopez Contreras

San Luis Potosi, S.L.P.
15 de mayo de 2026

Índice

1. Introduccion

La ciberseguridad no se limita al uso de herramientas tecnicas, analisis de logs o explotacion controlada de vulnerabilidades. Tambien exige criterio profesional para decidir que acciones son aceptables, cuales son proporcionales y cuales cruzan limites eticos, legales u organizacionales. Un especialista puede tener conocimiento y acceso suficiente para realizar una accion, pero eso no significa que este autorizado ni que sea correcto ejecutarla.

En esta actividad se analizan tres escenarios relacionados con acceso no autorizado interno, vulnerabilidad critica no reportada y uso indebido de informacion obtenida mediante OSINT. Para cada caso se identifica el dilema etico, la decision profesional recomendada, la justificacion desde tres enfoques eticos, los mandamientos de etica informatica involucrados y la clasificacion del tipo de delito cibernetico.

2. Objetivos

2.1. Objetivo general

Evaluar la capacidad para analizar, justificar y tomar decisiones eticas en escenarios reales de ciberseguridad, considerando marcos eticos, legales y organizacionales.

2.2. Objetivos especificos

1. Identificar dilemas eticos en operaciones de ciberseguridad.
2. Aplicar enfoques eticos utilitaristas, de derechos y del bien comun.
3. Relacionar decisiones profesionales con los mandamientos de la etica informatica.
4. Clasificar el tipo de delito cibernetico involucrado en cada escenario.
5. Justificar decisiones con criterio tecnico, legal y profesional.

3. Marco de analisis utilizado

Para evitar respuestas superficiales, cada escenario se analiza con la misma estructura. Esto permite demostrar criterio profesional y no solo opinion personal.

Criterio	Aplicacion dentro del analisis
Dilema etico	Se identifica el conflicto entre una accion tecnicamente posible y los limites eticos, legales u organizacionales.
Decision profesional	Se define que accion debe tomar un especialista responsable.
Etica utilitarista	Se evalua que decision genera menor dano y mayor beneficio colectivo.
Enfoque de derechos	Se revisa si se respetan privacidad, propiedad, autorizacion, debido proceso y confidencialidad.
Bien comun	Se analiza si la decision protege la confianza, continuidad y seguridad de la organizacion.
Mandamientos de etica informatica	Se relacionan las acciones con principios de uso responsable de tecnologia.
Clasificacion del delito	Se determina si corresponde a delito informatico, delito asistido por computadora o delito incidental.

Tabla 1: Estructura de analisis aplicada a los tres escenarios.

4. Referencia conceptual: mandamientos de etica informatica

Para esta actividad se consideran como referencia los principios conocidos como los diez mandamientos de la etica informatica. No se usan como una lista decorativa, sino como criterios para identificar que conducta se respeta o se vulnera en cada caso.

No.	Principio etico resumido
1	No usar la computadora para danar a otras personas.
2	No interferir con el trabajo informatico de otras personas.
3	No revisar archivos, correos o informacion ajena sin autorizacion.
4	No utilizar la computadora para robar.
5	No utilizar la computadora para levantar falso testimonio o enganar.
6	No copiar ni usar software sin pagar o sin licencia.
7	No usar recursos informaticos ajenos sin autorizacion.
8	No apropiarse del trabajo intelectual de otras personas.

No.	Principio etico resumido
9	Pensar en las consecuencias sociales de los programas, sistemas o acciones realizadas.
10	Usar la computadora con respeto, responsabilidad y consideracion hacia otros.

Tabla 2: Principios de etica informatica considerados para la evaluacion.

5. Escenario 01: Acceso no autorizado interno

Descripcion del escenario

Trabajas en el area de ciberseguridad de una empresa. Durante una revision de logs detectas que un companero accedio a correos privados del director general sin autorizacion. El companero argumenta que lo hizo para detectar posibles fugas de informacion.

5.1. Identificacion del dilema etico

El dilema consiste en decidir si se debe tolerar una accion no autorizada porque aparentemente buscaba proteger a la organizacion, o si se debe reportar porque vulnera privacidad, confidencialidad y controles internos. El punto central es que una finalidad de seguridad no justifica acceder a correos privados sin autorizacion formal, trazabilidad ni alcance definido.

La accion del companero cruza un limite claro: aunque pertenezca al area de ciberseguridad, no tiene derecho automatico a inspeccionar informacion privada o sensible. En seguridad informatica, el acceso debe basarse en autorizacion, necesidad operativa y procedimiento documentado, no en criterio individual.

5.2. Decision profesional

Decision recomendada

Como especialista, documentaria el hallazgo en los logs, preservaria la evidencia sin alterarla y reportaria el incidente al responsable correspondiente: lider de ciberseguridad, area legal, cumplimiento o recursos humanos, segun el protocolo interno. No confrontaria informalmente al companero ni ocultaria el evento.

La respuesta correcta no es encubrirlo ni justificarlo como una accion de buena intencion. Si realmente existia sospecha de fuga de informacion, debio solicitarse autorizacion formal, abrirse un caso interno y delimitarse el alcance de la revision.

5.3. Justificacion desde marcos eticos

Enfoque	Justificacion
Etica utilitarista	Reportar el incidente genera mayor beneficio para la organizacion porque protege la confianza interna, evita abusos futuros y permite investigar si existia una fuga real mediante un procedimiento legitimo. Tolerarlo crearia un precedente peligroso: cualquier empleado podria invadir informacion privada alegando una supuesta intencion de seguridad.
Enfoque de derechos	El director conserva derecho a privacidad, confidencialidad y proteccion de sus comunicaciones corporativas segun las politicas internas. El companero violo el principio de autorizacion y excedio sus permisos.
Bien comun	El bien comun organizacional exige que las investigaciones de seguridad sean trazables, autorizadas y proporcionales. La seguridad no puede sostenerse sobre abusos internos porque eso destruye la confianza en el area encargada de proteger la informacion.

Tabla 3: Justificacion etica del Escenario 01.

5.4. Mandamientos de etica informatica involucrados

En este escenario se vulneran principalmente los mandamientos 3, 7, 9 y 10. El mandamiento 3 se viola porque el companero reviso informacion ajena sin autorizacion; el 7 porque uso

recursos o accesos informaticos fuera del alcance permitido; el 9 porque no considero las consecuencias organizacionales y legales de su accion; y el 10 porque no actuo con respeto hacia la privacidad ni hacia los procedimientos institucionales.

5.5. Clasificacion del delito

La conducta se clasifica como **delito informatico**, porque el acto principal consiste en acceder sin autorizacion a informacion digital mediante sistemas informaticos. La computadora y los sistemas de correo no son solo herramientas secundarias; son el medio y el objetivo directo de la conducta indebida.

6. Escenario 02: Vulnerabilidad critica no reportada

Descripcion del escenario

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

6.1. Identificacion del dilema etico

El dilema consiste en elegir entre aprovechar una vulnerabilidad critica para beneficio personal o actuar conforme al alcance autorizado del trabajo profesional. Aunque el especialista tenga la capacidad tecnica de explotar la falla, no existe autorizacion contractual final ni permiso explicito para ejecutar acciones que afecten fondos, cuentas o activos financieros.

Este es el escenario mas grave de los tres porque combina conocimiento tecnico, oportunidad de abuso, ausencia de autorizacion formal y posible dano economico directo. En ciberseguridad, la diferencia entre una prueba legitima y un ataque real es la autorizacion verificable.

6.2. Decision profesional

Decision recomendada

No explotaria la vulnerabilidad para extraer dinero ni haria pruebas destructivas. Documentaria de forma responsable la evidencia minima necesaria para demostrar la existencia del hallazgo, detendria cualquier accion fuera de alcance y notificaria al canal autorizado para regularizar el contrato, definir alcance y establecer reglas de prueba.

La accion correcta es preservar la etica profesional y evitar cualquier conducta que pueda interpretarse como fraude, robo, extorsion o acceso no autorizado. Si no hay contrato final ni alcance firmado, el margen de actuacion debe ser conservador.

6.3. Justificacion desde marcos eticos

Enfoque	Justificacion
Etica utilitarista	No explotar la vulnerabilidad evita dano economico, dano reputacional, perdida de confianza y consecuencias legales. El mayor beneficio colectivo se obtiene reportando responsablemente el riesgo para que sea corregido.
Enfoque de derechos	El cliente tiene derecho a la proteccion de sus activos, fondos, sistemas y datos. Sin autorizacion contractual, el pentester no tiene derecho a manipular dinero ni ejecutar acciones que excedan una comprobacion controlada.
Bien comun	La profesion de ciberseguridad depende de la confianza. Si un especialista explota vulnerabilidades para beneficio personal, deteriora la legitimidad del pentesting y pone en riesgo a clientes, usuarios y al propio sector.

Tabla 4: Justificacion etica del Escenario 02.

6.4. Mandamientos de etica informatica involucrados

Si el especialista explota la vulnerabilidad para extraer dinero, se vulneran los mandamientos 1, 4, 7, 9 y 10. Se viola el 1 porque se causa dano a la organizacion; el 4 porque se usa la computadora para robar; el 7 porque se utilizan recursos informaticos sin autorizacion suficiente; el 9 porque se ignoran las consecuencias sociales, economicas y legales; y el 10 porque se actua sin responsabilidad profesional.

Tambien se respeta el sentido de estos mandamientos si el especialista decide no explotar la falla, documentarla y reportarla formalmente.

6.5. Clasificacion del delito

La conducta se clasificaria como **delito informatico**. La explotacion de la vulnerabilidad en un sistema financiero para extraer dinero seria un ataque directo contra un sistema informatico y sus activos. Tambien podria relacionarse con fraude o robo, pero dentro de las categorias solicitadas corresponde principalmente a delito informatico porque el sistema digital es el medio central del ataque.

7. Escenario 03: Uso de herramientas OSINT

Descripcion del escenario

Estas investigando a una persona sospechosa de fraude. Encuentras informacion personal en fuentes abiertas, como direccion, familia, habitos y datos similares. Tu superior te pide usar esa informacion para presionarlo psicologicamente.

7.1. Identificacion del dilema etico

El dilema consiste en decidir si se debe usar informacion obtenida de fuentes abiertas para intimidar o manipular psicologicamente a una persona sospechosa. Aunque la informacion sea publica o accesible, eso no autoriza su uso con fines de presion, amenaza, acoso o coercion.

OSINT no significa “todo se vale”. La recoleccion de informacion debe tener finalidad legitima, proporcionalidad, minimizacion de datos y apego al marco legal. Usar datos familiares, domicilio o habitos personales para presionar a alguien transforma una actividad de investigacion en una practica abusiva.

7.2. Decision profesional

Decision recomendada

Me negaria a usar la informacion personal para presionar psicologicamente a la persona. Limitaria el reporte a datos relevantes para la investigacion, eliminaria informacion excesiva o no necesaria, documentaria la solicitud indebida del superior y, si corresponde, escalaria el caso a cumplimiento, legal o al responsable etico de la organizacion.

La accion correcta es separar la investigacion legitima de la intimidacion. Si existen indicios de fraude, deben canalizarse mediante procedimiento formal, denuncia, analisis financiero o investigacion autorizada, no mediante presion psicologica.

7.3. Justificacion desde marcos eticos

Enfoque	Justificacion
Etica utilitarista	Usar informacion personal para presionar podria obtener una reaccion inmediata, pero genera mas dano que beneficio: riesgo de acoso, abuso de poder, dano a terceros y perdida de legitimidad de la investigacion. El mayor beneficio se logra usando canales formales.
Enfoque de derechos	La persona investigada conserva derechos de privacidad, dignidad, presuncion de inocencia y debido proceso. Que un dato sea publico no elimina la obligacion de tratarlo de forma proporcional y legitima.
Bien comun	El bien comun exige investigaciones confiables, no tacticas de intimidacion. Presionar psicologicamente con datos familiares o personales normaliza abusos y erosiona la confianza en los procesos de seguridad.

Tabla 5: Justificacion etica del Escenario 03.

7.4. Mandamientos de etica informatica involucrados

Se vulneran principalmente los mandamientos 1, 5, 9 y 10 si la informacion se usa para presionar o intimidar. El mandamiento 1 se relaciona con no causar dano; el 5 con no usar tecnologia para manipular, enganar o construir una narrativa abusiva; el 9 con considerar

las consecuencias sociales del uso de informacion personal; y el 10 con usar los sistemas con respeto y consideracion.

Tambien puede relacionarse con el mandamiento 7 si se emplean herramientas, cuentas o recursos institucionales para una finalidad no autorizada.

7.5. Clasificacion del delito

La conducta se clasifica principalmente como **delito asistido por computadora**. La informacion OSINT y las herramientas digitales funcionan como medios para facilitar una posible intimidacion, acoso, coercion o presion indebida. El delito no necesariamente consiste en vulnerar un sistema, sino en usar recursos digitales para facilitar una conducta abusiva contra una persona.

8. Comparativo general de los tres escenarios

Escenario	Dilema principal	Decision profesional	Clasificacion
Acceso no autorizado interno	Justificar o no una invasion de correos privados bajo el argumento de detectar fugas de informacion.	Preservar evidencia, reportar por canal formal y no encubrir el acceso indebido.	Delito informatico.
Vulnerabilidad critica no reportada	Aprovechar una falla financiera sin contrato final o actuar dentro de autorizacion profesional.	No explotar para extraer dinero; documentar evidencia minima y reportar formalmente.	Delito informatico.
Uso indebido de OSINT	Usar datos personales abiertos para presionar psicologicamente a una persona sospechosa.	Negarse a intimidar, limitar el reporte y escalar la solicitud indebida.	Delito asistido por computadora.

Tabla 6: Comparacion de dilemas, decisiones y clasificacion del delito.

9. Postura profesional final

Los tres escenarios muestran un mismo principio: en ciberseguridad, la capacidad tecnica no equivale a autorizacion etica ni legal. Acceder a correos privados, explotar una vulnerabilidad financiera o usar OSINT para presionar psicologicamente puede parecer util desde una vision inmediata, pero profesionalmente representa abuso de privilegios, ruptura de confianza y exposicion a consecuencias legales.

La decision correcta en los tres casos consiste en actuar con autorizacion, proporcionalidad, documentacion, minima invasion y escalamiento formal. Un especialista de ciberseguridad debe proteger sistemas y personas, no usar sus conocimientos como pretexto para invadir privacidad, robar activos o manipular individuos.

10. Conclusiones

El analisis de los tres escenarios permite concluir que la etica en ciberseguridad exige algo mas que saber identificar riesgos tecnicos. Tambien implica reconocer limites, respetar derechos y actuar conforme a procedimientos autorizados. El escenario de acceso no autorizado interno muestra que la seguridad no justifica revisar informacion privada sin permiso. El escenario de vulnerabilidad critica evidencia que un pentest sin autorizacion clara puede transformarse en delito si se explota el sistema. El escenario de OSINT demuestra que la informacion publica tambien puede utilizarse de forma abusiva si se emplea para intimidar o presionar.

En todos los casos, la respuesta profesional debe orientarse a documentar, reportar, limitar el dano y preservar la confianza. La ciberseguridad responsable no se basa en hacer todo lo que tecnicamente es posible, sino en hacer solamente lo que es autorizado, necesario, proporcional y defendible ante la organizacion, la ley y la sociedad.

Referencias

Computer Ethics Institute. (s. f.). *The Ten Commandments of Computer Ethics*.

Association for Computing Machinery. (s. f.). *ACM Code of Ethics and Professional Conduct*.

National Institute of Standards and Technology. (s. f.). *Computer Security Incident Handling Guide*.