Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

Propuesta de Programa de Prevención de Delitos (PPD) y Análisis de Responsabilidad Penal.

Caso UFV-LOGISTIA S.A.

Héctor Ramírez López

Índice

1. Introducción

El documento se ha elaborado desde el rol de Compliance Officer de UFV-LOGISTIA S. A. Una compañía especializada en servicios de logística industrial, con sedes operativas en Madrid y Barcelona.

1.1. Contexto

La organización afronta una brecha de seguridad importante. Se descubrió un empleado de sistemas instalando software ilegal sin permiso, en los ordenadores de la empresa. Esto facilitó a terceros el acceso remoto a servidores donde hay datos delicados de clientes.

De acuerdo con la investigación forense que se realizó este incidente tiene características agravantes:

- El acceso remoto no autorizado persistió activo por al menos 90 días, demasiado tiempo.
- Se ha confirmado el robo de datos sensibles de clientes.
- Hay posibilidad que terceros desconocidos estuvieran involucrados en la explotación de la vulnerabilidad.
- Hubo una falta de controles internos, además no existía un canal de denuncias para detectar esta irregularidad a tiempo.

  Importante hay que destacar si el empleado, aunque no tuviese permisos de administrador, el Departamento de TI fracaso en la supervisión, permitiendo estas acciones por tres meses.

1.2. Objetivo del informe

- Analizar la responsabilidad penal de UFV-LOGISTIA S: A. Respecto al código penal español.
- Diseñar un plan de prevención de delitos.
- Proponer medidas para corregir y prevenir futuros incidentes.

2. Identificación de delitos aplicables

- Descubrimiento y revelación de secretos
  - Al almacenarse información sensible en los servidores, seria revelación de secretos.
  - También el software que se instaló permitía el acceso a terceros por lo tanto personas no autorizadas accedieron a la información.

- Daños informáticos
  - Como el empleado hizo cambios en el servidor como instalar un software no autorizado.
  - Instalando este software comprometió la integridad permitiendo la entrada a terceros.
- Estafas / acceso a datos de clientes utilizado para engaño
  - Como se confirma que se robó información se podría utilizar para ataques de phising contra los clientes.
  - Para que exista estafa debe de haber intención de beneficiarse económicamente en este caso la participación de terceros y el robo de datos valioso los cuales se podrían vender o usarlos para fraudes bancarios.

2.1 Evaluación de la posible responsabilidad penal

El articulo 31 bis reconoce dos formas de imputar estos delitos que son la vía de los administradores y la vía de los subordinados en este caso aplicaría la de los subordinados.

El delito en este caso fue cometido por un empleado del área de sistemas, al ser un subordinado, la responsabilidad de la empresa depende de si existían mecanismos de control.

Para que la empresa fuese responsable de esto debe demostrarse que fallaron los controles en este caso:

- Falta de supervisión: Se indica que el departamento de TI no superviso sus actividades
- Ausencia de controles: Se indica que hubo falta de controles internos.
- Duración del fallo: El acceso no autorizado se mantuvo al menos 90 días.

En cuanto al beneficio directo o indirecto a primera vista parece que la empresa no se beneficia de ninguna manera, pero se habría podido beneficiar indirectamente por los ahorros de costes al no implementar herramientas de monitorización o al no tener un canal de denuncias y no dedicar recursos a la supervisión de los empleados.

2.2 Evaluación de posibles atenuantes

La empresa no puede librase totalmente de la pena, pero sí que puede reducirla llevando a cabo lo siguiente:

- Confesión de la infracción:
  - La empresa tiene que comunicar el delito a las autoridades competentes.
  - En el análisis forense interno ya se ha detectado el delito por lo que la empresa debería autodenunciarse proactivamente.

- Colaboración en la investigación:
  - Aportar pruebas nuevas para poder aclarar lo sucedido.
  - La empresa debe entregar el informe forense que demuestra el "acceso remoto no autorizado durante al menos 90 días" y facilitar la identificación del empleado, esto demuestra voluntad de no encubrir al culpable interno.

- Reparación del daño:
  - Reparar o disminuir el daño causado antes del juicio.
  - Al haber robo de información de clientes, la empresa debe notificar a los afectados, ofrecer servicios de protección de identidad si fuera necesario y asumir las posibles pérdidas económicas que los clientes sufran por este robo.

2.3 Propuesta de programa de prevención de delitos

1. Identificación de actividades de riesgo

Se realiza un análisis de las áreas donde se pueden cometer los delitos identificados en este caso (Descubrimiento de secretos, Daños informáticos).

- **Área de Sistemas (TI):** Riesgo alto. Actividades críticas: administración de servidores, gestión de privilegios de acceso remoto y mantenimiento de bases de datos.
- **Área Comercial/Atención al Cliente:** Riesgo medio-alto. Actividad crítica: tratamiento y almacenamiento de datos personales y bancarios de clientes.
- **Gestión de Compras/Proveedores:** Riesgo medio. Actividad crítica: contratación de servicios tecnológicos externos (para evitar la entrada de terceros maliciosos).

2. Protocolos de toma de decisiones y formación de la voluntad

Se establecen procedimientos para asegurar que las decisiones no se toman sin control.

- **Política de "Mínimo Privilegio":** Ningún empleado podrá auto concederse permisos de administrador sin la autorización de un superior.
- **Validación de Software:** Se prohíbe terminantemente la instalación de software no autorizado. Cualquier nueva instalación requerirá unas aprobaciones (Solicitud -> Evaluación de Seguridad -> Aprobación Técnica -> Instalación).
- **Segregación de Funciones:** Las tareas de administración de sistemas y las de auditoría de seguridad deberán recaer en personas o departamentos distintos.
- **Modelos de gestión de recursos financieros**

Aunque el incidente fue técnico, se requieren controles económicos para impedir la financiación de ilegalidades o el pago de sobornos.

- **Control de pagos a proveedores TI:** Auditorías de facturas para asegurar que no se paga por servicios de "soporte remoto" no autorizados.

- **Partidas presupuestarias para Compliance:** Asignación obligatoria de recursos financieros para la formación en ciberseguridad, mantenimiento del canal de denuncias y auditorías externas.

3. Sistema Disciplinario

Mecanismo para sancionar el incumplimiento del modelo (Art. 31 bis.5. 4º CP).

- Se añade al Convenio Colectivo y al contrato laboral unas clausulas específicas de ciberseguridad.
- **Graduación de sanciones:**
  - *Leve:* Compartir contraseñas no críticas.
  - *Grave:* Instalación de software no autorizado sin perjuicio.
  - *Muy Grave:* Deshabilitar antivirus, facilitar acceso remoto a terceros o vulnerar secretos de empresa.

4. Canal de Denuncias

Elemento que no existía en el momento del incidente.

- **Implementación:** Creación de un canal digital accesible (web y correo) para empleados y terceros.
- **Garantías:** Se garantiza el anonimato, la confidencialidad y la protección ante represalias para el denunciante.
- **Gestión:** Recepción y filtrado por parte de un gestor externo independiente para asegurar la objetividad, con reporte directo al Órgano de Cumplimiento.

5. Supervisión y Verificación (Órgano de Cumplimiento y Auditoría)

- **Designación del Compliance Officer:** Se formaliza el nombramiento de un responsable o comité con poderes autónomos de iniciativa y control.
- **Auditoría Periódica:** El modelo se verificará anualmente. Además, se establece una verificación extraordinaria inmediata tras el incidente para asegurar que la brecha de seguridad ha sido cerrada.
- **Monitorización Tecnológica:** Implementación de un SIEM para auditar logs y detectar accesos inusuales en tiempo real.

2.4. Propuesta de sistema de Gestión compliance UNE 19601

La utilidad de la norma UNE 19601 se basa en tres fases críticas que fallaron durante el incidente:

1. **Prevención (Antes del delito):**

   La norma obliga a realizar un análisis de riesgos. Si UFV-LOGISTIA hubiera tenido este sistema, el riesgo de la instalación de software no autorizado habría estado identificado y prohibido mediante controles bloqueantes y políticas.

2. **Detección (Durante el delito):**

   a. El incidente actual permaneció oculto durante 90 días por falta de vigilancia. La UNE 19601 exige controles de monitorización y un canal de denuncias efectivo. Su utilidad consiste en reducir el tiempo de exposición, permitiendo detectar irregularidades como picos de tráfico de datos o accesos remotos inusuales.

3. **Reacción (Después del delito):**

   Establece protocolos claros de respuesta ante incumplimientos. Esto asegura que ante un futuro incidente la empresa sepa cómo asegurar pruebas forenses, iniciar una investigación interna y notificar a las autoridades inmediatamente, facilitando el acceso a poder reducir las penas.

Adoptar la UNE 19601 aporta ventajas estratégicas y jurídicas fundamentales tras el incidente:

- **Prueba de Diligencia Debida:** La certificación por un tercero independiente sirve como evidencia robusta ante un tribunal de que la empresa ha cumplido con sus deberes de supervisión.
- **Recuperación Reputacional:** Tras el robo de datos de clientes, la confianza en la marca está dañada. La certificación UNE 19601 envía un mensaje al mercado y a los clientes de que la empresa se ha reformado y ahora opera bajo los más altos estándares éticos y de seguridad.
- **Alineación con el Código Penal:** Garantiza que el Programa de Prevención de Delitos (PPD) diseñado cumple con todos los requisitos del art. 31 bis, evitando vacíos legales que podrían dejar indefensa a la organización.

Aparte la une19601 ayuda a separar la responsabilidad de la empresa de la del empleado.

2.5. Integración con Sistema antisoborno ISO 37001

Como el incidente de seguridad colaboro activamente un empleado interno y también terceros externos, es fundamental integrar la norma ISO 37001 para prevenir que el personal técnico sea sobornado para facilitar accesos ilegítimos.

El sistema se compone de cuatro apartados fundamentales:

1. Evaluación de Riesgos de Corrupción

Se analizaron las áreas donde existe mayor probabilidad de soborno en UFV-LOGISTIA S.A

- **Riesgo de Soborno Pasivo en TI:** Se identifica como un riesgo alto que los administradores de sistemas reciban pagos, regalos o favores de ciberdelincuentes a cambio de credenciales o instalación de puertas traseras.
- **Riesgo en la Cadena de Suministro:** Posibilidad de sobornos en la selección de proveedores tecnológicos por ejemplo comprar software no legitimo a cambio de cobrar comisiones.

2. Medidas Antisoborno y Políticas Preventivas

Normas claras para prohibir conductas de riesgo

- **Política de Tolerancia Cero:** Prohibición absoluta de aceptar regalos, invitaciones o pagos, para el personal con acceso a datos sensibles.
- **Diligencia Debida:** Investigación obligatoria de la reputación de cualquier tercero o socio comercial antes de darle acceso a los sistemas de la empresa.

3. Controles Financieros y Formación

Herramientas para detectar el flujo de dinero ilegal y concienciar al personal.

- **Controles Financieros:** Implementación de auditorías y segregación de funciones en los pagos siempre firmado por dos personas para evitar que se camuflen pagos de sobornos.
- **Formación y Concienciación:** Talleres obligatorios para el personal de TI sobre las consecuencias penales del delito de corrupción. El empleado debe saber que aceptar dinero por instalar un software es un delito de corrupción.

4. Nombramiento del responsable de Cumplimiento Antisoborno

Quién vigila que esto se cumpla

- Se designa formalmente un responsable de Cumplimiento Antisoborno.
- Para garantizar su eficacia, este cargo tendrá independencia y autoridad respecto a la Dirección General, reportando directamente al órgano de gobierno. En el caso de la empresa esta función se integrará dentro de las competencias del *Compliance Officer* para juntar la vigilancia penal y antisoborno.

3. Preguntas de reflexión

1. ¿Puede la persona jurídica ser condenada aunque no se identifique al autor físico?

Si según el artículo 31 del código penal que indica que la responsabilidad de la empresa es autónoma y no es necesario identificar al empleado, con poder demostrar que el delito se cometio dentro de la empresa ya valdria.

2. ¿Qué elementos del art. 31 bis?5 CP son más difíciles de aplicar en el ámbito TIC?

La supervisión del funcionamiento. Es difícil aplicar con el personal de TI, ya que los administradores de sistemas tienen privilegios para casi todo y conocimientos técnicos suficientes para borrar sus huellas o alterar los registros, dificultando que un auditor no técnico pueda detectar sus infracciones.

3. ¿Qué peso tiene la formación en la prevención de delitos informáticos?

Tiene un peso bastante importante ya que gran parte de los incidentes son causa del error humano.

4. ¿Qué conexiones observas entre Compliance y Ciberseguridad?

El compliance define las obligaciones legales y los riesgos a evitar mientras que la ciberseguridad implementa las medidas técnicas para evitar los posibles riesgos.

5. Señala tres ejemplos concretos de controles de prevención que propondrías.

1. **Monitorización SIEM:** Un sistema que analiza los registros en tiempo real y lanza una alerta si detecta tráfico inusual como una conexión abierta durante 90 días seguidos.
2. **Autenticación Multifactorial (MFA) para Acceso Remoto:** Obligar a usar un segundo factor para cualquier conexión remota (VPN/RDP). Esto dificulta el acceso de terceros desconocidos, aunque tengan la contraseña.
3. **Gestión de Cuentas Privilegiadas (PAM):** Sistema que controla, limita y graba las sesiones de los administradores de sistemas para evitar abusos de poder.

Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

RAMIREZ LOPEZ HECTOR - 53858461M

Firmado digitalmente por RAMIREZ LOPEZ HECTOR - 53858461M
Fecha: 2025.12.03 11:34:48 +01'00'