La importancia de la ciberseguridad en la empresa. Compliance. La otra protección (interna y externa)

Carlos Soucase

16 de mayo de 2021

Vulnerabilidades externas

- Las empresas deben cuidarse de ser víctimas de **ataques externos** de personas que buscan acceder a sus datos para obtener un provecho o como parte de un ejercicio de hacking para poner a prueba la seguridad informática (hacking "ético" o malicioso, según el caso).

Thousands of students in Germany queue for email access

18 December 2019 Share

There will be queues at the university throughout the week, as 38,000 students seek a new email password

Some 38,000 students in Germany have been asked to queue in person for a new email password, after their university was hit by a cyber-attack.

The students at Justus Liebig University (JLU) Giessen have been asked to provide proof of identity in person because of "legal requirements".

The attack, on 8 December, initially took the entire university offline.

It told students it was investigating the incident with the help of Germany's Research Centre for Cyber Security.

"All employees and students have to collect their new personal password personally," the university **said in a statement**.

Students have been asked to bring an ID card to the university's gym at an allotted time determined by their birth date.

According to the published schedule, it will take a full five days to process all students.

BROSETA

Vulnerabilidades externas

Cyber ataque. Protección de datos (sensibles)

- Las empresas deben evitar que su propio personal incurra **en infracciones por acción u omisión** que pongan en peligro los sistemas (activar ramsonware, etc)

Rouen hospital turns to pen and paper after cyber-attack

21 November 2019 Share

Hospitals have become a popular target for cyber-criminals

A cyber-attack on a hospital in Rouen last week caused "very long delays in care", reports the AFP news agency.

Medical staff at the French city's University Hospital Centre (CHU) were forced to abandon PCs as ransomware had made them unusable, a spokesman said.

Instead, staff returned to the "old-fashioned method of paper and pencil", said head of communications Remi Heym.

No patients were endangered as a result of the cyber-attack, the hospital said, in a statement **published on Facebook**.

Vulnerabilidades externas

Cyber ataque. Protección de datos (sensibles)

Therapy patients blackmailed for cash after clinic data breach

By Zoe Kleinman
Technology reporter

26 October 2020

Many patients of a large psychotherapy clinic in Finland have been contacted individually by a blackmailer, after their data was stolen.

The data appears to have included personal identification records and notes about what was discussed in therapy sessions.

Vastaamo is a nationwide practice with about 20 branches and thousands of patients.

The clinic has advised those affected to contact the police.

It said it believed the data had been stolen in November 2018, with a further potential breach in March 2019.

BROSETA

EL PAÍS

ESPAÑA

ANDALUCÍA CATALUÑA C. VALENCIANA GALICIA MADRID PAÍS VASCO MÁS COMUNIDADES TITULARES »

SUCESOS ›

La EMT de Valencia sufre una rocambolesca estafa de cuatro millones de euros

Una directiva transfiere la suma a una cuenta externa tras ser víctima presuntamente del fraude del CEO

IGNACIO ZAFRA

Valencia - 28 SEP 2019 - 13:42 CEST

Estafa ¿quién tiene poderes y firmas?

Fila en una parada de autobús en Valencia. MÒNICA TORRES

La Empresa Municipal de Transportes (EMT) de Valencia ha informado este viernes de que ha sufrido una estafa rocambolesca. Su jefa de administración transfirió entre el 3 el 20 de septiembre cuatro millones de euros a una cuenta bancaria en Hong Kong creyendo que participaba en una operación confidencial de la compañía pública, cuando en realidad, según fuentes cercanas a la investigación, estaba siendo una víctima de la conocida como estafa del CEO (consejero delegado).

BROSETA

Vulnerabilidades externas

Secreto empresarial ¿cómo se protegía?

Un producto capilar que puede salir muy caro

Olaplex, una 'start up' californiana, decidió demandar a L'Oréal en 2016 por robar sus secretos comerciales, incumplir un contrato e infringir dos patentes relacionadas con un producto para la protección del cabello durante los tratamientos de decoloración. La pequeña compañía acusaba a L'Oréal de haber sustraído sus secretos en una reunión comercial, mientras que la francesa aseguraba haber ideado, de forma independiente en 2014, el componente controvertido. Tras años de litigio, el jurado popular de un tribunal de Wilmington (Delaware) determinó que la actuación de la multinacional de cosméticos fue intencional y el juez ordenó que L'Oréal indemnizara a la 'start up' con 81,5 millones de euros. La francesa anunció directamente que recurriría este fallo.

Vulnerabilidades externas

I+D
Códigos fuente
¿cómo se accedió?
¿Ausencia de NDA?

Conseguir billetes de avión al mejor precio

Uno de los asuntos nacionales con mayor controversia y directamente relacionado con los secretos empresariales es el que ha enfrentado a la empresa española Trappit con American Express (Amex). La causa, que ha pasado por diferentes fases de instrucción y que todavía no se ha resuelto, investiga la presunta copia por parte de la estadounidense de 'Arpo', un algoritmo desarrollado por Trappit que monitoriza en tiempo real el precio de los billetes de avión para encontrar el mejor. La española siempre ha afirmado que mantuvo conversaciones con Amex para la comercialización de este sistema, momento en el que esta última empresa tuvo acceso a los códigos fuente del programa y, supuestamente, gracias a cuyos secretos pusieron en marcha su propia herramienta Lastfare.

Vulnerabilidades internas

PROTECCIÓN DE LA INFORMACIÓN

- ✓ Uno de los primeros elementos que debe resguardar la empresa son los datos propios y de terceros que maneja, particularmente los datos personales e información sensible que puede generarle responsabilidad conforme lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
  - ✓ La empresa deben contar con medidas de seguridad ajustadas, y acordes al tipo de información almacenada. En este sentido, para el caso de datos especialmente sensibles, deberán implementarse mecanismos de encriptación, uso de servidores propios, restricción y control de acceso acordes con el nivel de riesgo.

- ✓ Revelación de datos, se hace especial distinción entre los que afectan a la intimidad personal y los que los que se refieren al acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos a la intimidad personal.

Vulnerabilidades internas

- ✓ **HARDWARE**: otro riesgo que debe mitigarse dentro de las empresas es la utilización de los recursos informáticos propios para actividades delictivas o con el fin de ocasionar daños a terceros.

- ✓ **SOFTWARE**: existe el riesgo de que el personal o colaboradores hagan uso de programas o aplicaciones ilegales en sistemas de la empresa, consciente o inconscientemente. Si la empresa obtiene un beneficio de este tipo de actividades (por ejemplo, la utilización de un software descargado ilegalmente para la gestión), puede generarse responsabilidad penal para la persona jurídica.

Vulnerabilidades internas

Espionaje

Una química que conoce la fórmula de la Coca-Cola

El pasado 22 de abril, el Tribunal de Distrito Este de Tennessee condenó a una trabajadora de Coca-Cola por cometer espionaje empresarial y sustraer secretos comerciales de la fórmula de los recubrimientos de las latas de bebidas. Xiaorong You, una ciudadana estadounidense de origen chino, trabajó como ingeniera principal de la multinacional y fue una de las pocas personas que tuvo acceso a los secretos comerciales logrados en una investigación global de Coca-Cola. Según explica el fallo, la trabajadora, antes de abandonar su puesto en la compañía de Atlanta, copió archivos en un disco duro externo con el único objetivo de crear una nueva empresa competidora de recubrimientos de latas en China.

BROSETA

Vulnerabilidades internas

Robo de propiedad industrial y empresarial

Martes 18 | MAYO 2021 | Nº 92

Dieciocho meses de cárcel por robar a Google

Anthony Levandowski, ingeniero de profesión, fue denunciado por Google por la supuesta apropiación ilícita de secretos empresariales sobre el proyecto del vehículo autónomo desarrollado por el gigante estadounidense. El trabajador, que se enfrentaba a 33 cargos por robo de propiedad intelectual e industrial, llegó a un acuerdo de culpabilidad con el Ministerio Público el pasado mes de agosto. El tribunal le sentenció a cumplir 18 meses de prisión y a entregar una compensación económica de más de 621.000 euros. Meses después, el expresidente de EEUU Donald Trump firmó su indulto, junto al de muchos otros, justo antes de dejar la Casa Blanca.

BROSETA

El compliance como elemento protector

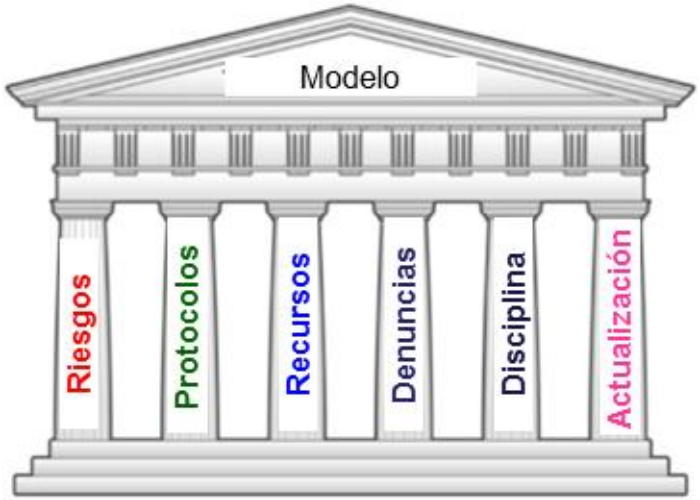
En consecuencia todas las empresas, con independencia de su tamaño y sector están viviendo esta revolución, no exenta de riesgos, ya que pueden ocurrir conductas, **con o sin conocimiento de la alta dirección** de la empresa, que se contemplan en el Art-31 bis del Código Penal y de los que se deriva responsabilidad penal a la persona jurídica es el **Delito informático** y el **Delito de Descubrimiento, revelación de secretos y allanamiento informático**.

Las empresas deben hacer un esfuerzo por proteger sus infraestructuras y garantizar la fiabilidad de sus datos. Para ello la empresa deberá contar con la asesoría de especialistas en materia de seguridad informática, que determinen cuáles medidas son recomendables y qué herramientas de control se deben implementar.

Modelo de Prevención de Responsabilidad Penal de la Persona Jurídica

Modelo: 6 elementos

+



Norma Española
UNE 19601
Mayo 2017

Órgano de cumplimiento

Promover e Implantar

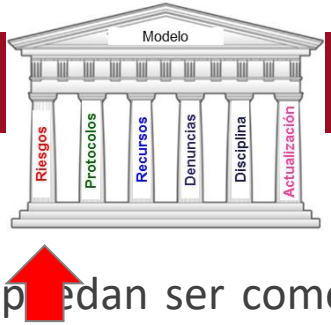
Supervisar

Vigilar

Controlar

BROSETA

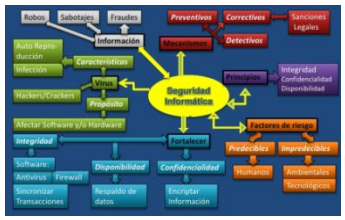
Modelo de prevención: mapa de riesgos



La identificación de las **actividades** en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos es una de las partes fundamentales en el compliance.

Elaborar un **mapa de riesgos** que corresponda a la realidad de cada organización sirve para entender qué controles se deben implantar para prevenir y mitigar los posibles riesgos, así como monitorizar la eficacia de tales controles, es una labor de gran importancia en este ámbito.

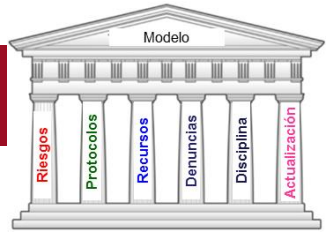
✓Planes de continuidad de negocio: análisis riguroso de las actividades y las infraestructuras con el objeto de implantar controles y procedimientos que mitiguen la probabilidad de ocurrencia de tales desastres.



✓ Mapas de seguridad: permiten levantar riesgos y diseñar un plan de seguridad desde el diseño, que garantice el cumplimiento de las medidas de seguridad informática exigidas en el Reglamento Europeo de Protección de Datos, en la Directiva UE 2016/1148 del Parlamento Europeo y del Consejo de 6/7/16 de Ciberseguridad.

BROSETA

Modelo de prevención: protocolos y procedimientos



Establecimiento de los **protocolos o procedimientos** que comprenden el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquellos.

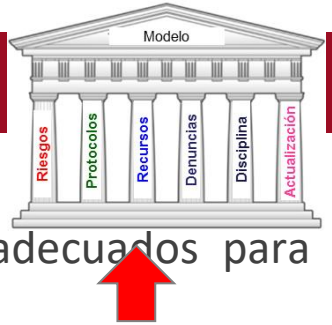
La conducta de la organización ante los riesgos éticos y de compliance inherentes a su cadena de valor, será determinante para su nivel de cumplimiento, su desempeño y su rentabilidad

- ✓ Código ético o de conducta
  - ✓ Código ético informático
  - ✓ Definición de modelos de gobierno y gestión de seguridad de la información, basados en ISO 27001
  - ✓ Redacción de Cuerpo Normativo de Seguridad (políticas, estándares, procedimientos gestión- DLP, IRM, MDM…)

- ✓ Definición de Plan Director de Seguridad (IT+OT)
- ✓ Políticas Corporativas de la Seguridad de la Información: Para proteger los secretos de empresa, para evitar o perseguir el espionaje empresarial, los daños y las estafas informáticas, para establecer política de actualizaciones y copias de seguridad, con una adecuada Política Corporativa, que organice la información de la empresa, niveles de acceso y uso, para controlar la información estratégica de la empresa.

BROSETA

Modelo de prevención: recursos financieros



Disponer de modelos de gestión de los **recursos financieros** adecuados para impedir la comisión de los delitos que deben ser prevenidos.

- ✓ Asesoría externa:
  - ✓ Asesoría externa en seguridad informática

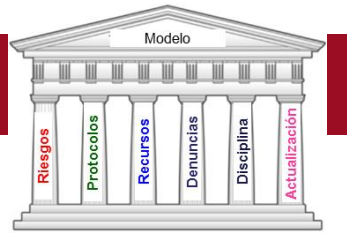
  - ✓ Software Asset Manager (SAM)

  - ✓ Data protection Officer (DPA)

  - ✓ Formación y concienciación: Es muy importante que las compañías conciencien y formen a sus trabajadores, y sobre todo en temas de ciberseguridad ya que es una brecha de acceso para los ciberdelincuentes.

  - ✓ Utilización de herramientas de Data Analytics para gestión de fraude: Para detectar y evitar el fraude y las pérdidas económicas que causan.
- ✓ Tomar <u>medidas proactivas</u>: reducirán los costes por ataques, y mejorarán la posición de la seguridad en la compañía y en consecuencia su imagen y reputación

Modelo de prevención: canal denuncias



Imponer la **obligación de informar** de posibles riesgos e incumplimientos al órgano encargado de vigilar el funcionamiento y observancia del modelo de prevención.

- ✓ Establecimiento de un canal de comunicación (whistleblower line). Se trata de un sistema de comunicación que permite a todas las personas vinculadas a la empresa (socios, directivos, trabajadores, en algunos casos proveedores y hasta clientes) presentar denuncias y también sugerencias sobre el cumplimiento normativo ante el encargado o responsable de la gestión del canal (oficial de cumplimiento). Este canal debe proteger al denunciante de buena fe garantizando cierto anonimato y asegurar indemnidad ante posibles represalias

- ✓ Herramientas de canal de denuncias:

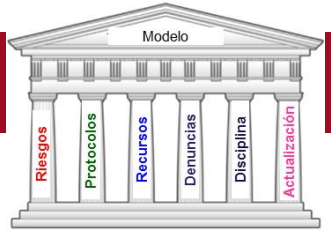
  -propias: Confidencialidad/Encriptación/Sellado de tiempo

  -externalizado: ¿Quién? ¿Alguien la ha verificado/testado?

  -LOPD: ¿sabemos dónde están alojados los datos?

BROSETA

Modelo de prevención: disciplina

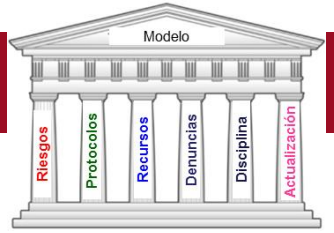


Establecer un **sistema disciplinario** que sancione adecuadamente el incumplimiento de las normas.

- ✓ De acuerdo y respetando los Convenios de los trabajadores y sectoriales
- ✓ Debe distinguir a los que cumplen con las políticas y normas de la empresa de los que no
- ✓ El sistema disciplinario puede sancionar y también destacar a aquellos que cumplan.
- ✓ Ojo al Procedimiento:
  - ✓ diligencias debidas en las obtención de evidencias de incumplimientos (ej. abrir un portátil de un empleado, monitorizar su comunicaciones, etc.) que son técnicas y de procedimiento,
  - ✓ donde el Compliance Officer:
    - ✓ 1) debe asesorar previamente,
    - ✓ 2) debe velar y supervisar que se proceda correctamente
    - ✓ 3) debe proponer la adopción de medidas disciplinarias/sanciones.

BROSETA

Modelo de prevención: actualización



Realizar una **verificación periódica** del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

- ✓ Definición de Matrices de Control y Cuadros de Mando para Gobiernos de TI:
  Para determinar la eficiencia de los controles de seguridad.

- ✓ Realización de auditorías internas de sistemas

- ✓ Ejecución de Auditorías de Sistemas (Comunicaciones, Seguridad, Desarrollo…):Informe auditor de seguridad de sistemas de información que comprende el análisis y gestión de sistemas para identificar las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de redes de comunicaciones o servidores.

BROSETA

csoucase@broseta.com
649410181
963921006