Convergencia de modelos de tres líneas de defensa entre IT y OT

Erik de Pablo Martínez

Mayo 2022

Charlas técnicas 2022

ISACA®
ADACSI | Buenos Aires Chapter

¿QUIÉN SOY?:

- Erik de Pablo Martínez, físico por la Univ. Autónoma de Madrid y PDD por el IESE.
- Tiene una dilatada experiencia en automatización de procesos industriales y en SSII, desarrollada en la industria del petróleo, en España y en Sudamérica. Está orientado a la auditoría de sistemas en entornos industriales y de negocio y focalizado en los nuevos riesgos tecnológicos: ciberseguridad, infraestructuras críticas, detección y prevención del fraude, IoT, IA, Big Data, Blockchain etc…
- Recientemente y durante 6 años ha sido Director de Investigación en **ISACA-Madrid** y es socio Director de la empresa de auditoría de sistemas RUTILUS
- Es CISA (Certified Information System Auditor) y CRISC (Certified in Risk and Information Systems Control).
- Contacto: edepablo@rutilus.com

Índice

Introducción

- El pasado mes de mayo de 2021 se produjo un importante ciberataque sobre una infraestructura crítica en EEUU, el conocido ataque sobre **Colonial Pipeline**. Una organización que soporta un oleoducto de más de 8.000 km que distribuye combustible desde Texas a Nueva Jersey. La compañía pagó un rescate de 5 millones de dólares.
- El presidente Biden tuvo que declarar la emergencia nacional y disponer alternativas para mitigar el impacto que produjo el desabastecimiento de gasolinas durante varias semanas.
- Por otra parte, la reciente experiencia con los ataques a la cadena de suministro de **Solar Winds** puso sobre la mesa que centenares de empresas industriales, entre otras, habían sucumbido a un sofisticado ataque, bien diseñado y de larga duración, detectado en diciembre de 2020.

- Esta empresa provee software a 300.000 clientes en todo el mundo, incluyendo el Ejército de EE.UU., el Pentágono, el Departamento de Estado, de Comercio, el de Tesoro y la Oficina presidencial.
- El software afectado se utiliza ampliamente para gestionar las redes internas en los sectores de la electricidad, el petróleo y el gas y en la industria manufacturera
- Apenas recuperados del susto, sucedió el ataque a Colonial Pipeline.

Introducción -2

- Resulta sorprendente que estos ciberataques hayan tenido éxito cuando parecía que se habían desplegado iniciativas eficaces para evitarlos. La sensación más extendida era que, gracias a la intensa regulación sobre ciberseguridad que se había impuesto en estos últimos años, las compañías habían cumplido sus obligaciones y por lo tanto deberían estar libres de peligro. Y no ha sido así.
- ¿Cuál es la causa de este fallo?
- ¿Qué se puede hacer?
- Intentaremos presentar una visión sobre el estado de situación y propondremos una aproximación para adaptar e implantar el conocido modelo de “Tres líneas de defensa” en el entorno de las infraestructuras críticas industriales.

Análisis de un escenario -IT

- En una empresa industrial típica de cierto tamaño, el CISO (responsable de ciberseguridad IT) es una figura que suele estar en el nivel 3 (o más probablemente 4) de la jerarquía de la empresa, lo que dificulta extraordinariamente que sus preocupaciones y necesidades lleguen a la Alta Dirección.
- Consecuencias:
  - Es probable que el CISO no tenga interlocutores válidos a su nivel, dado el bajo escalón de su puesto. La mayoría de los directivos que manejan las Operaciones, tanto comerciales como industriales, se encuentran en un par de escalones por encima de él y normalmente no atienden ni comprenden sus demandas de atención.
  - El CISO puede encontrarse con dificultades para explicar a la Alta Dirección que los riesgos en ciberseguridad son crecientes y que ello conlleva un presupuesto progresivo (no-lineal), con una curva acentuada, siguiendo el patrón de agresividad creciente de las amenazas. Esto se traducirá en que la capacidad de los recursos del CISO se aleje gradualmente de lo necesario.
- Pero además, el CISO, una vez resignado a la falta de interlocución, debe proteger su puesto, por lo que es habitual que apantalle el problema y decida mostrar a la alta dirección que “no hay excesivos riesgos”.
- Este comportamiento, muy arriesgado, está muy extendido entre los CISOs actuales.

Análisis de un escenario -OT

- Por otra parte, la historia reciente indica que preocupación de los CISO ha sido exclusivamente el área de informática corporativa (IT). Esa es su procedencia profesional y su foco de interés exclusivo
- Esto significa que habitualmente no hay apenas nada en su agenda relacionado con el área OT, probablemente por estas dos causas:
  - El área OT es muy reacia a considerar a los “informáticos” como interlocutores, debido a su escaso conocimiento de la “componente de proceso industrial” de su actividad y existe una aversión histórica para trabajar conjuntamente. Ello ha provocado en esa empresa varias escaramuzas entre ambos equipos, que han fracasado y que IT recuerda.
  - Además, el área IT, efectivamente, no tiene ninguna experiencia en los procesos industriales y cumple sobradamente con las malas expectativas de OT
- Esta situación está mejorando en los últimos años y lo más probable es que se hayan realizado varios proyectos conjuntos para mejorar la ciberseguridad OT. Pero el problema no se ha terminado de arreglar, porque IT sigue sin tener nociones de procesos industriales. Es decir, en realidad el acercamiento se ha producido desde OT hacia IT.

Análisis de un escenario -OT (2)

- OT no suele tener una figura equivalente al CISO. A lo sumo tiene un responsable de “Instrumentación y Control”, o con algún nombre similar, que se encuentra aún más abajo que el CISO en jerarquía.
  - Todavía no ha calado entre los responsables de operaciones el hecho de que hoy en día la ciberseguridad (*security*) es tanto o más importante que la seguridad industrial clásica (*safety*).
  - Por ejemplo, cuando se revisan los mapas de riesgo que los responsables de operaciones realizan sobre sus instalaciones, los riesgos asociados a la ciberseguridad suelen ser increíblemente bajos. Incomprensiblemente los resultados de pérdidas esperadas a 5 años no alcanzan ni el 1% del valor de la instalación.
- Con estas premisas es muy difícil que la persona que incluye entre sus cometidos la ciberseguridad OT, pueda hacer llegar a la alta dirección sus necesidades y su percepción del riesgo.
- Se podría decir que es una tormenta perfecta, ni por parte de su posición en la organización ni por parte de una hipotética colaboración con IT se da el escenario para tratar adecuadamente la ciberseguridad industrial.

Relación entre IT y OT

- La introducción hace un par de décadas de tecnologías populares, como Windows, en el entorno industrial ha supuesto una revolución que ha aproximado el entorno industrial al mundo de la informática corporativa.
  - Ello ha facilitado enormemente la interconexión entre ambos entornos.
  - A partir de entonces ha sido sencillo enviar y actualizar el parte diario de producción.
  - Y se podía recibir la planificación actualizada que el área Logística estuviera diseñando.
  - Además, con ello se ha podido simplificar y unificar el protocolo de comunicaciones alrededor del TCP/IP

- Todo han sido ventajas, …… salvo por la aparición en OT de las amenazas de ciberseguridad.

Relación entre IT y OT -2

- La interconexión se realizó entre dos equipos que seguía pegados a sus respectivas organizaciones, sus tareas y sus objetivos.
- El problema ha surgido al intentar coordinar la protección global de la empresa ante las nuevas amenazas de ciberseguridad.

- Como conclusión, tenemos dos equipos sensibilizados ante el problema de la ciberseguridad, que han atacado el problema y han implantado diferentes aproximaciones a modelos de control, pero manteniendo una cierta independencia en su gestión.

Teoría del modelo de “Tres líneas de defensa”

- El Modelo de las Tres Líneas de Defensa es un modelo creado en 2013 por la “*European Confederation of Institutes of Internal Auditing*”, el ECIIA.
  - La IIA lo adoptó formalmente en la declaración de posición “Las tres líneas de defensa en gestión de riesgos y control eficaces” publicada en 2013 y adaptada de la Guía emitida por ECIIA/FERMA sobre la 8.a Directiva de Derecho de Sociedades de la UE (artículo 41).
- El modelo tiene en su base elementos procedentes de la separación de responsabilidades, también denominado “Segregación de funciones”.
- Se trata de un enfoque muy extendido en los países anglosajones y consiste en aplicar la idea de que ningún grupo organizativo tenga la capacidad total de diseñar y realizar actividades sin que exista ningún control externo.
- Esta idea ha dado lugar al sistema de contrapesos o de poder balanceado que se utiliza normalmente en la “*segregation of duties*”.

Teoría del modelo de “Tres líneas de defensa” -2

- En este caso, la separación se realiza sobre tres actividades:
  - Ejecutar las actividades y los controles que mitigan sus riesgos
  - Diseñar los controles que mitigan los riesgos
  - Revisar si el diseño de los controles y su ejecución son adecuados y se llevan a cabo de forma regular
- El mismo nombre de “Tres líneas de defensa” nos hace alusión a una especie de fortaleza en la que se hubieran dispuesto 3 anillos o murallas consecutivas que impidieran un ataque con éxito.
- En realidad, se trata de la división de un conjunto de responsabilidades con objeto de asegurar que su funcionamiento final sea el correcto y el esperado.
  - Si para evitar que un riesgo se exprese es necesario implantar unos controles mitigatorios, el hecho de que su definición y su implantación fueran efectuados por las mismas personas pudieran dar lugar a errores “sistémicos”.
  - A ello habría que agregar que nadie aseguraría que tales controles estén funcionando continuamente.

Teoría del modelo de “Tres líneas de defensa” -3

- Por ello se establece una división:
  1. La Primera Línea serían aquellas funciones de la organización encargadas de la operativa en el día a día, son los responsables de evaluar y por lo tanto mitigar los riesgos. Por ello se responsabilizan de implantar los controles.
  2. La Segunda Línea serían todas aquellas funciones tales como control interno y gestión de riesgos que diseñan y supervisan la implantación de actividades de control interno y gestión de riesgos por parte de la Primera Línea.
  3. La Tercera Línea sería auditoría interna, que asegura de forma independiente la efectividad del control interno y de la gestión de riesgos, realizados tanto por las Primera Línea como por la Segunda Línea.

ISACA
ADACSI | Buenos Aires Chapter

Teoría del modelo de “Tres líneas de defensa” -4

- Este es el enfoque teórico que se presentó en el año 2013.
- Se ha aplicado y difundido mucho desde entonces, pero siempre en el ámbito de la denominada “informática corporativa”.
- No existen apenas referencias de que se haya aplicado de forma estructurada en un entorno de Control Industrial.

Teoría del modelo de “Tres líneas de defensa” -5

- En el año 2020 el IIA ha actualizado el modelo de Tres Líneas de Defensa.
- El nuevo modelo se organiza alrededor de seis principios:

1. Estructurar el gobierno de la organización para rendir cuentas, definir acciones, asegurar y asesorar.
2. Establecer los roles dentro del órgano de gobierno para que funcione de forma eficaz. Es necesario alinear los objetivos y actividades a los intereses de cada parte.
3. Definir responsabilidades para alcanzar objetivos tanto en primera como segunda línea. Las funciones de la primera línea están directamente alineadas con la entrega del producto o servicio. La segunda línea se encarga de la asistencia en la gestión de riesgos.
4. Establecer los roles de tercera línea como la auditoría interna. Este principio también sirve para asesorar a los demás órganos para asegurarse del cumplimiento de los objetivos.
5. La auditoría interna es independiente de las responsabilidades de la dirección para ser totalmente objetiva y creíble.
6. Creación y protección del valor. Todas las funciones trabajan colectivamente con el objetivo de alinearse y lograr los intereses de todas las partes involucradas.

Modelo de “Tres líneas de defensa” en OT

- Una conclusión que hemos sacado es que el modelo de Tres líneas de defensa puede ser efectivamente aplicado en el entorno OT.

- Nuestra propuesta es que no solo puede hacerse, sino que sería muy conveniente aplicarlo.
  - En particular, el modelo que proponemos tiene mucho más sentido cuando una organización industrial está digitalizándose.

Modelo de “Tres líneas de defensa” en OT -2

- Consideremos una organización industrial de tamaño medio.
  - Es muy probable que su organización OT haya hecho gran parte de su tarea, haya realizado un análisis de riesgos y que incluso haya desarrollado y adaptado un modelo de control para alinearse con las mejores prácticas.
  - Por ejemplo, siguiendo el estándar ISA99/IEC62443 (“Security for industrial automation and control system“), el marco norteamericano NIST (“Framework for Improving Critical Infrastructure Cybersecurity”, versión 1.1) o la (“Guía SGCI para el responsable de construir un Sistema de Gestión de la Ciberseguridad Industrial”) publicada por el Centro de Ciberseguridad Industrial.
  - Es posible que solo haya sido una adaptación de mínimos, pero en cualquier caso podría decirse que han implantado un “modelo” de control.
  - Si no lo ha tenido que hacer obligada por la normativa PIC lo habrá hecho porque este enfoque está presente en todas las publicaciones actuales y se da por supuesto en la literatura técnica.

Modelo de “Tres líneas de defensa” en OT -3

- Sin embargo, aún suponiendo que se hayan confeccionado esos modelos de control y que se hayan implantado, la organización OT está lejos de alcanzar un grado de excelencia en su proceso.
- Siguiendo el esquema de la figura adjunta, una organización en la fase descrita se encontraría en el nivel 3.
  - Esto quiere decir que no se han establecido procesos de revisión del modelo, revisión del mapa de riesgos, verificación del buen funcionamiento de los controles implantados ni existe un esquema de aprendizaje sobre los errores que se cometen y se detectan en su aplicación.

ISACA
ADACSI | Buenos Aires Chapter

Modelo de “Tres líneas de defensa” en OT -4

- En el área OT, sin embargo, ni en la regulación relativa a la Protección de Infraestructuras críticas (en España la Ley PIC) ni en las regulaciones europeas (Directiva NIS) se recoge nada más allá de la implantación de los controles mitigatorios de los análisis de riesgo realizados. No se menciona una auditoría sistemática sobre ellos.
- En concreto, en los Planes de Protección Específicos que se elaboran por cada Infraestructura Crítica Específica, solamente se deben detallar los siguientes tres capítulos:

1. Organización de la seguridad.
    a) En el PPE se debe constar quién son los Delegados de Seguridad para la infraestructura
    b) Además, debe constar con quién se debe coordinar el plan
2. Descripción de la infraestructura.
3. Resultado del análisis de riesgos:
    a) Medidas de seguridad (tanto las existentes como las que sea necesario implementar) permanentes, temporales y graduales para las diferentes tipologías de activos a proteger y según los niveles de amenaza declarados a nivel nacional.
    b) Plan de acción propuesto (por activo).

- Concluimos que los modelos de control que se hayan podido desarrollar consistirán en unos controles, que posiblemente estén funcionando, pero sobre los que no hay un plan sistemático de evaluación y *feed-back*.

Modelo de “Tres líneas de defensa” en OT -5

Proponemos que en el área OT se adapte una versión del modelo de Tres líneas de defensa que permita alcanzar un grado de madurez superior al actual y asegure que la mitigación de riesgos esté funcionando de manera eficaz.

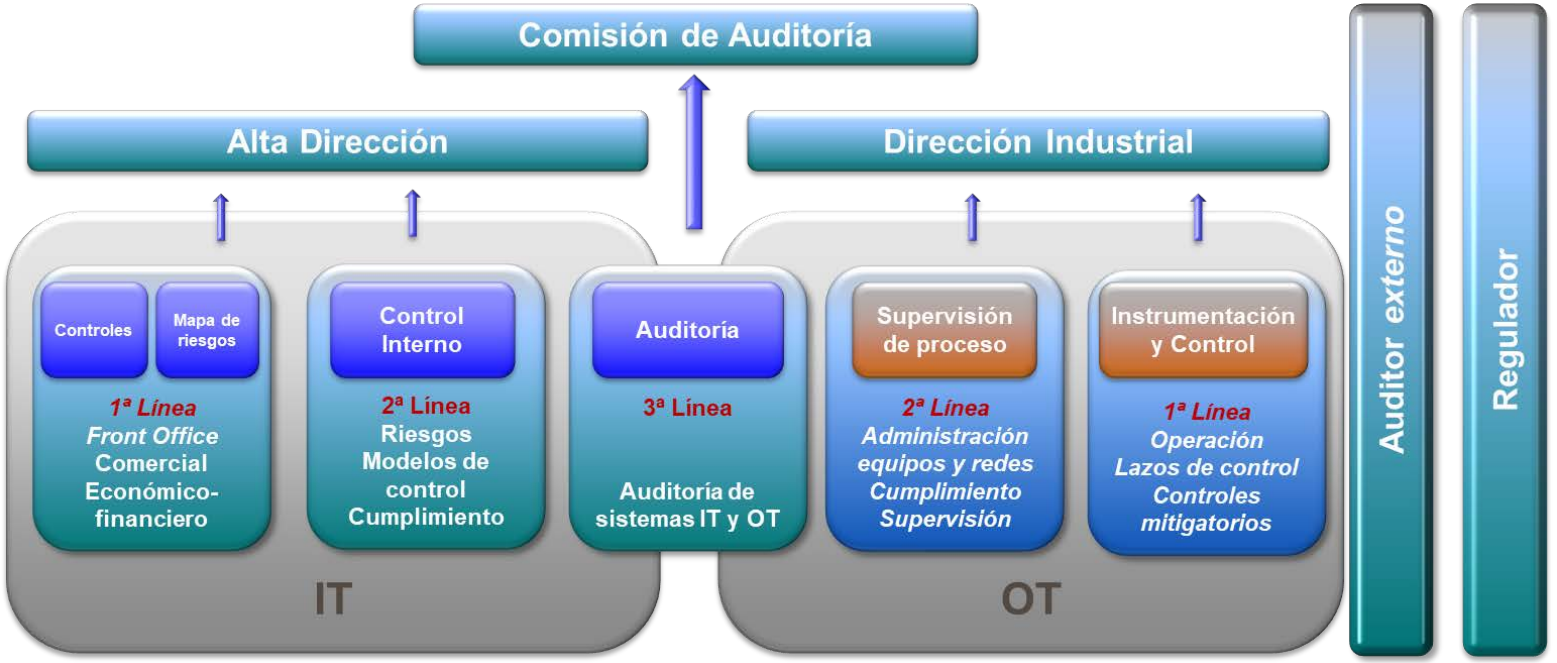
Modelo de “Tres líneas de defensa” en OT -6

- Para ello mostramos un posible esquema de actuación hacia el que se puede avanzar:

1. Suponemos que en la compañía existe un área de Auditoría especializada en Sistemas de Información que actúa como tercera de línea de defensa en lo tocante a la informática corporativa (IT). Este equipo podemos denominarlo para este propósito como “Auditoría de Sistemas”. En muchas organizaciones este grupo no existe, aunque es muy necesario y en tal caso convendría crearlo.
2. También damos por hecho que existe un equipo dedicado a revisar los mapas de riesgo y los modelos de control de la compañía, incluidos los de IT, actuando por lo tanto como segunda línea de defensa. Este equipo podemos denominarlo “Control Interno”.
3. Por su parte en OT existirá un equipo dedicado a mantener el estado de los sistemas de control, programar los lazos de control, mantener la instrumentación e implantar las medidas de protección de riesgos. Este equipo podemos denominarlo “Instrumentación y control”.
4. Es muy probable que en el área OT exista un grupo, quizás reducido, encargado de la “Supervisión del proceso”. Es un grupo que no realiza directamente la operación del proceso, pero supervisa el buen funcionamiento de los sistemas de control de proceso. Según los casos se denomina “ingeniería del proceso” o “control avanzado”, y podría asumir la revisión de los modelos de control y asegurar que los controles son efectivos.

Modelo de “Tres líneas de defensa” en OT -7

1. Crear un grupo específico dentro de la organización OT, paralelo a “Control Interno”, que podría denominarse “Control de riesgos y cumplimiento”, que podría estar englobado en “Supervisión de proceso” y de cometido:
   a) Confeccionar los mapas de riesgos de ciberseguridad OT
   b) Diseñar y mantener el diseño de la arquitectura básica de la red OT
   c) Revisar y adecuar el esquema de administración de los equipos y redes OT en coordinación con “Control Interno”
   d) Asegurar que el esquema definido cubre las exigencias de la regulación

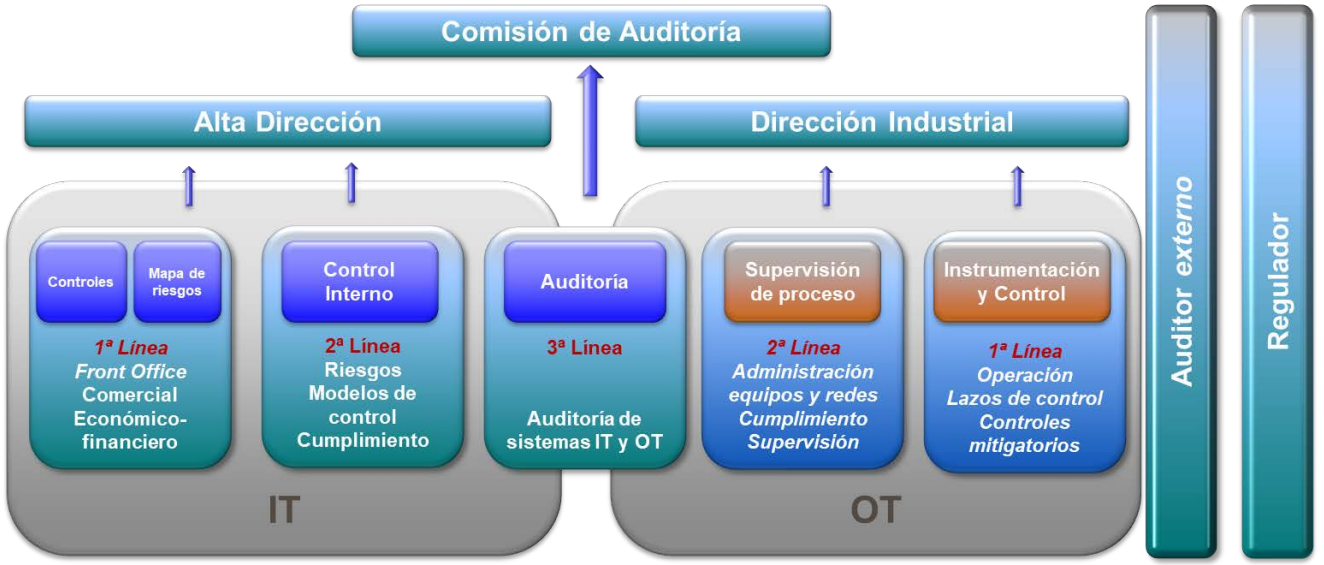


ISACA
ADACSI | Buenos Aires Chapter

Modelo de “Tres líneas de defensa” en OT -8

2. Organizar un equipo que se denominará “Auditoría de Sistemas Industriales” e incluirlo en Auditoría de Sistemas, si es que este último existe y si no es así crearlo.

   - Este equipo tiene que estar razonablemente formado en técnicas de control industrial, para que pueda hacerse cargo de las auditorías periódicas sobre los modelos de control.



ISACA
ADACSI | Buenos Aires Chapter

Modelo de “Tres líneas de defensa” en OT -9

3. Tareas:
   a) Revisar la metodología empleada en la elaboración del Mapa de Riesgos industrial (OT)
   b) Analizar el Modelo de Control implantando y su adecuación a la exposición de la instalación
   c) Revisar el buen funcionamiento de los controles implantados
   d) Concluir sobre el grado de exposición al riesgo de la instalación industrial.
   e) Elevar las conclusiones a la Dirección de la Instalación y al Comité de Auditoría (si existe).
   f) Tener disponible los informes para su posible revisión por parte del Regulador.

ISACA
ADACSI | Buenos Aires Chapter

Conclusiones - Coordinación entre IT y OT

- Con esta estructura organizativa podríamos tener dos equipos dedicados a la auditoría de los modelos de control, corporativo e industrial

  - Facilitaría la necesaria coordinación en los trabajos de diseño de controles y de auditoría
  - Permitiría extraer conclusiones generales sobre los riesgos globales de ciberseguridad en la empresa.
  - Prepararía la organización para redistribuir las responsabilidades en función de riesgos transversales, por ejemplo en la administración de la red

Reporting y asesoría en tecnología

- Una de las principales características de las nuevas tecnologías es que poseen una elevada complejidad y su evolución es muy rápida, por lo que es muy difícil tener un criterio actualizado sobre las mismas.
- Por ello, a diferencia de otros procesos de la compañía, la Alta Dirección necesita un asesoramiento al respecto para identificar carencias y riesgos no asumibles.
- El problema, un clásico de la segregación de funciones, es que hasta ahora esta asesoría ha sido realizada por personal directivo de las mismas áreas afectadas, áreas IT y OT, lo que conlleva un riesgo en sí mismo derivado de que no exista una visión imparcial o no comprometida con acciones realizadas o en curso.

Reporting y asesoría en tecnología -2

- Por ello que consideramos que el área de Auditoría, más concretamente el área de auditoría de sistemas, debería ofrecer una visión independiente y de alto nivel sobre el grado de madurez de los procesos informáticos tanto de IT como de OT, el nivel de cobertura de los riesgos y su posible impacto en la sostenibilidad de la compañía.
- Todo ello con objeto de que la Alta Dirección tenga una visión estratégica objetiva y en consecuencia puede establecer los planes correspondientes de remediación.
- Si bien este enfoque se distancia aparentemente del clásico sobre la independencia de Auditoría, aporta valor al mostrar todos los hechos significativos desde la perspectiva del grado de madurez.
- Consideramos que este enfoque moderno es una consecuencia del papel cada vez mas importante de los procesos de digitalización en las organizaciones.

Muchas gracias por su atención.

Charlas técnicas 2022