Desafíos de gobierno de TI para la gestión de dispositivos IoT en los entornos tecnológicos empresariales

IT government challenges for managing IoT devices in entrepreneurial technologic environments

Luis Alejandro Aburto Hernández,*
Instituto Politécnico Nacional
laburtoh0800@alumno.ipn.mx
ORCID: 0000-0001-7862-5359

Dra. Pilar Gómez Miranda,
Instituto Politécnico Nacional
pgomezm@jpn.mx
ORCID: 0000-0002-1480-3061

Recibido 09, febrero, 2024 Aceptado 26, abril, 2024

Resumen

La creciente adopción de tecnologías físicas, conocidas como IoT (Internet of Things) en los entornos tecnológicos empresariales ha provocado que los directores de tecnologías de información (CIOs por sus siglas en inglés) trabajen continuamente para incluir estos nuevos activos físicos en el modelo de gestión y gobierno corporativo. A través de una investigación descriptiva el presente documento tiene el objetivo de hacer un recuento de los riesgos que el uso de esta tecnología introduce en los ambientes de control organizacionales, así como el involucramiento que la alta dirección debe tener para abordarlos. La investigación muestra que regulaciones internacionales como el Reglamento General de Protección de Datos emitido por la Unión Europea y la ley Sarbanes-Oxley, por mencionar algunas, son legislaciones que introducen riesgos de cumplimiento a las organizaciones. Concluyendo con la necesidad del trabajo en conjunto de los CIOs con los directores de finanzas y directores ejecutivos para adoptar mejores prácticas de gestión y diseñar un marco de control extendido hacía estos dispositivos. Identificando como trabajo futuro el desarrollo de un modelo de gobernanza optimizado para los dispositivos IoT.

Palabras clave: IoT; gobierno de TI; control interno; cumplimiento

Abstract

The growing adoption of physical technologies, better known as IoT (Internet of Things) in enterprise technology environments has derived into CIOs continuous work to include these new physical assets in the management and corporate governance model. Through descriptive research the present manuscript aids to revisit the risks that the use of this technology introduces into organizational internal control environments and the top management involvement needed to address them. Research shows that international regulations such as the General Data Protection Regulation (GDPR) issued by the European Union and the Sarbanes-Oxley act (SOX), to mention a few, are laws that might cause compliance risks to businesses. Conclusion reached showed that CIOs but also finance directors and executive directors must pay attention to adopt better management practices and design an extended control framework towards these devices. An IT governance model is identified as future work, which needs to be specifically oriented to IoT devices.

Keywords: IoT; IT governance; internal control; compliance.

*Autor corresponsal

1. INTRODUCCIÓN

El Internet de las cosas (IoT por sus siglas en inglés) de acuerdo con (Chanal & Kakkasageri, 2020) es la red de objetos físicos, es decir, dispositivos, vehículos, electrodomésticos y otros artefactos dotados con capacidad computacional y de comunicación que les permite conectarse entre sí e intercambiar datos a través de la infraestructura de Internet global existente, por lo tanto, gracias a la basta disponibilidad de potentes procesadores, sensores automáticos, robots industriales y entornos de aprendizaje automático actualmente cualquier dispositivo puede ser inteligente, estar conectado a la red y ser capaz de capturar datos y enviarlos, lo que amplía el abanico de posibilidades que las organizaciones de hoy tienen para buscar la automatización de la producción, la eficiencia en la cadena de valor o ¿por qué no? innovar para crear nuevas fuentes de ingresos que beneficien al negocio. Lo anterior lo vemos reflejado ampliamente en el concepto de Industria 4.0 que de acuerdo con (Manavalan & Jayakrishna, 2019) es una combinación de tecnología digital, que transforma la producción industrial al siguiente nivel, donde la plataforma fundamental para el éxito de este nuevo paradigma es la revolución en tecnologías que consiste entre otras, en los dispositivos IoT.

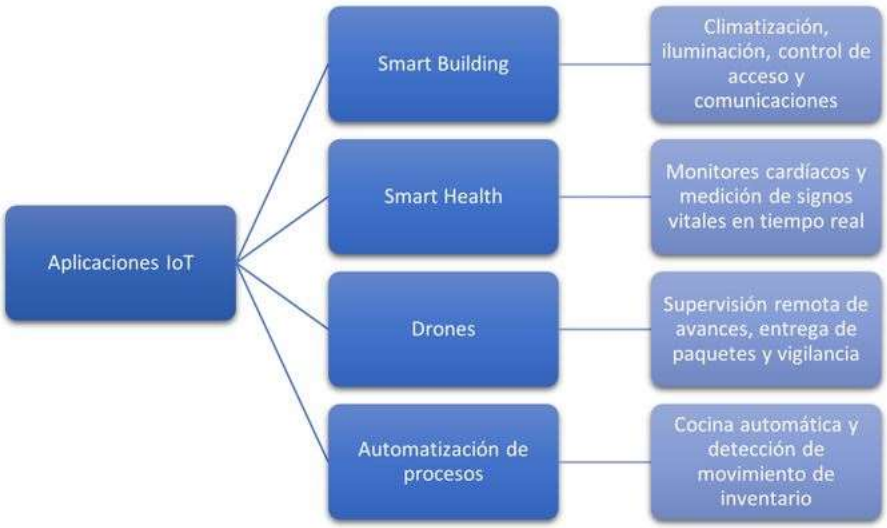
De acuerdo con el informe (State of the IoT 2020, 2020) publicado por IoT Analytics, el número total de dispositivos conectados a nivel mundial se espera que alcance los 30.9 mil millones para 2025, con un crecimiento anual del 21% en comparación con los 12.6 mil millones de dispositivos que se observaron en 2020, en este mismo sentido, la investigación (The Internet of Things: Mapping the Value Beyond the Hype, 2015) de McKinsey Global Institute, estima que el valor económico potencial generado por el IoT en distintos sectores industriales podría alcanzar entre 3.9 y 11.1 billones de dólares al año para 2025. Estos datos nos revelan una tendencia al alza en el uso y adopción de esta tecnología en los ambientes tecnológicos empresariales, este aumento acelerado ha causado que la visión de gestión y gobierno de los CIOs (Chief Information Officer, por sus siglas en inglés) se esté ampliando una vez más para incluir estos nuevos activos físicos en el modelo de gestión y gobierno de TI, de acuerdo con (Shokoohyar et al., 2020) el gobierno de TI es una de las disciplinas de liderazgo más críticas requeridas para permitir que las organizaciones alcancen sus objetivos operativos y estratégicos, donde un enfoque de gobierno basado en riesgos en el ambiente tecnológico que soporta las operaciones de la corporación, es la punta de lanza de los accionistas y otras partes interesadas para la toma de decisiones que les garantice la consecución de los resultados comerciales deseados. Bajo este panorama, a medida que la oferta del internet de las cosas se expande y la variedad de activos físicos disponibles en el mercado crece en conjunto con sus capacidades de procesamiento, se deja de manifiesto la necesidad de extender las buenas prácticas de gestión y gobierno de TI hacía estos dispositivos que claramente están tomando un rol protagónico en la operación de las organizaciones y la realización de sus objetivos.

Durante décadas, los responsables de las áreas de TI dentro de las organizaciones han centrado sus esfuerzos en la gestión y gobierno de tecnologías de comunicación, entornos de desarrollo, aplicaciones, marcos y metodologías de trabajo, ecosistemas de datos y otros elementos pertenecientes al componente digital de las TI, mientras que históricamente, el componente físico de los entornos tecnológicos ha sido mucho menos dinámico y se reduce principalmente a puntos de acceso e infraestructura de centros de datos, los cuales han evolucionado tecnológicamente hablando, pero su gestión y gobierno se han mantenido hasta cierto punto sin diferencias sustanciales a través de los años, sin embargo hoy en día observamos dispositivos inteligentes que de acuerdo con un estudio de (Pivoto et al., 2021) y (Malik et al., 2021) van desde monitores cardíacos en hospitales (Smart Health), drones con reconocimiento de imágenes para la inspección remota del avance en la construcción de infraestructura (carreteras, edificios, etcétera) hasta sensores inteligentes en las oficinas que activan o desactivan las amenidades del edificio (Smart Building) o cocineros robotizados en restaurantes que

miden perfectamente las cantidades a utilizar de ciertos ingredientes para preparar un platillo (Figura 1).

Figura 1

Aplicaciones de IoT en las industrias



Fuente: Elaboración propia

Estos ejemplos comprueban que las tecnologías digitales más avanzadas se están integrando en una nueva generación de dispositivos físicos inteligentes que están permitiendo con mayor frecuencia y a mayor escala la operación de procesos de negocio críticos para las organizaciones, incluso para aquellas que su negocio no se encuentra en la oferta de bienes y/o servicios relacionados con las TI.

Esta evolución del componente físico de los entornos de TI empresariales introduce nuevos retos para las organizaciones, los cuales no solo deben ser abordados por los CIOs sino también por los directores de finanzas (CFOs) y directores ejecutivos (CEOs), quienes deben repensar el modelo de gestión de servicios de TI proporcionados por estos dispositivos, así como la estrategia de gobierno a la que éstos deben ser sujetos para mantener un ambiente de control saludable al interior de la organización. De acuerdo con la investigación realizada por (Brockmann et al., 2018), los CEOs y CFOs de una organización tienen un rol preponderante en el gobierno y gestión de dispositivos IoT, inclusive desde antes de la puesta en marcha del ambiente basado en esta tecnología, por ejemplo, un CEO deberá establecer una visión y estrategia organizacional que tome partido en la adopción y el uso de dispositivos IoT, esto implica comprender las oportunidades y los desafíos que los dispositivos IoT pueden representar, y definir cómo la organización, de manera holística, puede aprovecharlos para lograr sus objetivos comerciales. Lo anterior sin dejar de lado que el CFO debe ser el responsable de la gestión financiera del proyecto de implementación de tecnología IoT en la organización, lo cual implica evaluar los costos asociados con la implementación y el mantenimiento de los dispositivos IoT, así como identificar las fuentes de financiamiento adecuadas, inclusive el CFO deberá evaluar el retorno de la inversión y la rentabilidad del proyecto con la finalidad de respaldar y asegurar una toma de decisiones informadas. Y en conjunto CIO, CEO y CFO serán los responsables de evaluar y gestionar los riesgos asociados con la implementación de dispositivos IoT en la organización. Considerando aspectos como la seguridad de los datos, la privacidad, la integridad de la red y la protección contra ciberataques. Todas las partes deberán trabajar en colaboración para desarrollar mecanismos de gobierno y estrategias de mitigación de riesgos robustas que den respuesta a cada uno de los retos de seguridad que representa el componente físico para asegurar una implementación efectiva y segura de los dispositivos IoT,

estableciendo canales de comunicación claros que promuevan una cultura organizacional que valore la innovación, la eficiencia y la seguridad.

Los dispositivos IoT se han convertido poco a poco en un aspecto vital de las organizaciones y es recientemente visto como una oportunidad estratégica para obtener una ventaja competitiva en relación con los otros actores del mercado. Cada proyecto de cada organización ha generado valor y mejoras que se traducen en beneficios económicos para las organizaciones que deciden implementar este tipo de tecnología. De manera general algunos de los beneficios que hacen esta tecnología tan atractiva para las organizaciones son:

- Eficiencia operativa: Los dispositivos IoT pueden mejorar la eficiencia en los procesos empresariales al automatizar tareas, recopilar datos en tiempo real y optimizar el uso de recursos. Esto puede resultar en ahorros de costos significativos y una mayor productividad.
- Reducción de costos: Los dispositivos IoT ayudan a las organizaciones a reducir costos en áreas como lo son el mantenimiento preventivo, la gestión de inventario, la energía y los gastos operativos, dado que permiten un monitoreo en tiempo real basado en datos, identificando problemas y realizando acciones correctivas de manera temprana, previniendo costosos fallos o interrupciones en la operación.
- Mejora de la toma de decisiones: Los dispositivos IoT generan grandes volúmenes de datos en tiempo real, lo que proporciona a las organizaciones una mayor visibilidad y conocimiento de sus operaciones, promoviendo una toma de decisiones informada.

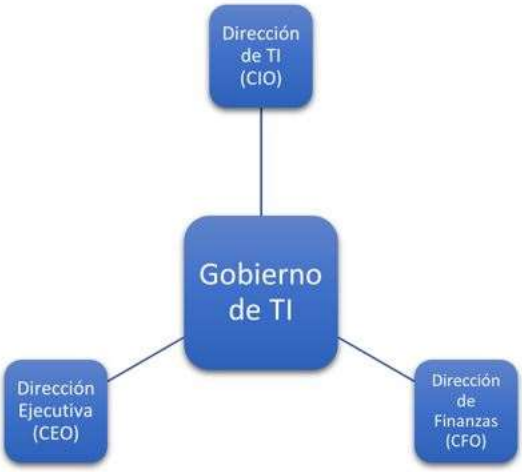
Los puntos anteriores muestran que el creciente interés de las empresas en la implementación de estos dispositivos y la definición de un modelo de gobierno de TI están respaldados por el gran impacto que esta tecnología tiene o puede tener dentro de las organizaciones.

Actualmente el gobierno de TI emplea conceptos de gobierno corporativo para impulsar y controlar estratégicamente las TI, en particular con respecto a dos pilares fundamentales: el valor que proporciona la TI a una organización y el control y la mitigación de los riesgos relacionados con la TI. El diseño de un modelo de gobierno consistente y bien definido ayuda a los accionistas y otras partes interesadas en la toma de decisiones, asegurando que las organizaciones logren sus objetivos comerciales específicos e inclusive describiendo cómo se lograrán esas metas y objetivos. ISACA en la última versión de COBIT define el gobierno de TI como el marco de trabajo, principios y políticas, estructuras, procedimientos, prácticas, información, habilidades, cultura, ética y comportamiento utilizados para establecer la dirección y monitorear el cumplimiento y el desempeño de la empresa de acuerdo con su propósito general y los objetivos definidos (ISACA, 2018). En otras palabras, el gobierno de TI es la definición de un modelo de rendición de cuentas, responsabilidad y toma de decisiones (entre otros elementos) que asegura que la inversión tecnológica de la organización permita la implementación de la estrategia de negocio de una manera efectiva y eficiente.

La alineación entre tecnología y objetivos de negocio hace evidente que el involucramiento de CIOs, CEOs y CFOs es crucial para llevar a buen puerto la implementación de un modelo de gobierno de TI (Figura 2) que incluya los dispositivos físicos inteligentes o en el caso de organizaciones que ya cuentan con un modelo de gobierno de TI, será requerido hacer una ampliación de este modelo para proveer gobierno a los dispositivos físicos inteligentes que se están sumando al ambiente tecnológico para cubrir las necesidades actuales de la organización.

Figura 2

Colaboración en el Gobierno de TI



Fuente: Elaboración propia

Esta ampliación de acuerdo con (Shokoohyar et al., 2020) se puede basar en numerosos marcos de trabajo como COSO, COBIT e ISO 38500 los cuales proporcionan lineamientos para los directores de organizaciones (incluidos dueños, miembros de la junta, directores, socios, altos ejecutivos y otros colaboradores) sobre el uso eficaz, eficiente y aceptable de la tecnología de la información dentro de sus organizaciones, estos marcos de trabajo han probado ser efectivos como guías en la implementación de modelos de gobierno TI y que sin lugar a duda son un excelente punto de partida para abordar los riesgos introducidos por esta nueva ola de dispositivos físicos inteligentes. Para los fines perseguidos por el presente trabajo no se entrará en detalle en la aplicación de alguno de los marcos de trabajo mencionados anteriormente para la implementación o ampliación de un modelo de gobierno de TI.

2. DESARROLLO

¿Cómo los dispositivos IoT puede introducir nuevos retos en el gobierno de TI?

Las regulaciones y los estándares relacionados con el gobierno de los dispositivos físicos y como éstos hacen uso de los recursos de red de una empresa o como recaban y protegen información personal de clientes, proveedores y empleados pueden ser desconocidos y desafiantes para la dirección de TI, sin mencionar que éstas permanecen en constante cambio a través de los años con base en los avances tecnológicos que se manifiestan día con día.

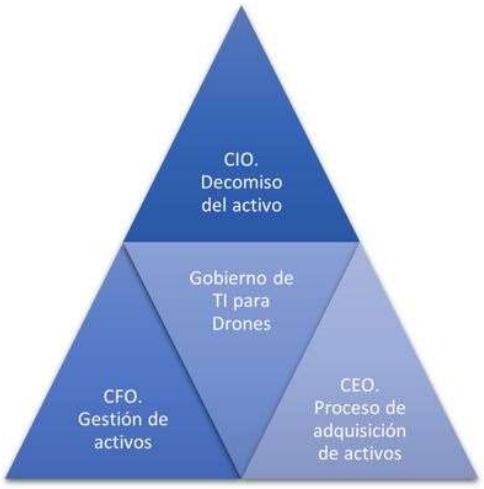
Por tal motivo es necesario mantener un constante monitoreo en las regulaciones que puedan tener un impacto en la gestión y uso de dispositivos inteligentes físicos para la generación de valor en las empresas, por ejemplo, tan solo en Estados Unidos se estimaba que para el año 2020 el número de drones con aplicaciones civiles como monitoreo remoto de infraestructura y entrega de paquetes rondaría los 2.7 millones (Tian et al., 2019), por lo que con miras en la gestión del tráfico aéreo, las organizaciones en EE. UU. que utilizan o piensan implementar drones como una solución de valor para la entrega automatizada de paquetes, deben registrarlos y obtener la autorización de espacio aéreo de la Administración Federal de Aviación de EE. UU, inclusive en algunos casos y dependiendo del tipo de dispositivo, los drones deben de estar equipados con un sistema inalámbrico de identificación que les

permitan ser reconocidos por los radares de la entidad reguladora para evitar ser derribados (Syd Ali, 2019).

El involucramiento de activos físicos, como los drones, en la operación de las organizaciones conlleva la inclusión de estos activos, financieramente hablando, en la gestión de activos fijos de la compañía (Brous et al., 2020) y lo que esto implica (vida útil, depreciación, obsolescencia, etcétera) y tecnológicamente hablando será necesario diseñar un plan de reemplazamiento del activo, en el cual se incluyan procesos para revocar certificados o identificadores, extraer y archivar datos que se encuentran almacenados en el dispositivo, así como eliminación de los datos que se consideren sensibles. Este punto de gestión de activos establece el vínculo entre la figura de administración del departamento de TI (CIO) y las figuras de dirección ejecutiva (CEO) y dirección financiera (CFO), ya que el riesgo de una gestión inapropiada de activos de TI no solo tiene un impacto a nivel dirección de TI sino también a nivel organizacional en su conjunto. Observamos de esta manera, la aplicación holística y extendida que el uso de esta tecnología genera en los entornos empresariales, donde la implementación de procesos de gobierno adecuados a las necesidades de la organización no es un tema que deba ser abordado de manera aislada por el CIO, sino que se debe contar también con el involucramiento apropiado del CEO y CFO de la compañía para la toma de decisiones (Figura 3).

Figura 3

Ejemplo de actividades de gobierno TI



Fuente: Elaboración propia

Por otro lado, en un entorno tecnológico con presencia de dispositivos físicos inteligentes en el que se procesan cantidades impresionantes de datos es de esperarse que entre estos datos se encuentren datos personales y sensibles, por lo que al igual que sucede con los sistemas de información empresariales, es prioridad garantizar la privacidad de éstos cuando son recolectados y procesados por dispositivos físicos inteligentes. Por tal motivo los CIOs deben considerar en la definición del gobierno de TI la figura propietaria de los datos y metadatos producidos por estos dispositivos (Wachter, 2018), que ayude a resolver cuestionamientos como los siguientes ¿quién legalmente podrá copiar, distribuir o procesar modelos de comportamientos basados en estos datos y metadatos? ¿Quién lo debe controlar? Es necesario de la misma manera considerar en el modelo de gobierno de TI que los dispositivos físicos inteligentes basados en sensores y cámaras suelen recopilar y compartir datos continuamente, muchas veces sin el conocimiento o permiso explícito del usuario final, por ejemplo, una imagen o un fragmento de video, mediante técnicas de inteligencia artificial, se pueden usar para identificar a una persona, lo que automáticamente etiqueta estos datos como datos personales por lo

que deben de recopilarse y protegerse en consecuencia o de otra manera se podría materializar el riesgo de un tratamiento inadecuado de datos personales.

Es conveniente mencionar que otro reto en el gobierno y gestión de dispositivos IoT radica en la dificultad de asegurar, desde un punto de vista de seguridad de la información, estos dispositivos físicos inteligentes debido a que con frecuencia se fabrican con sistemas operativos y protocolos de comunicación genéricos, los cuales integran pocas o nulas características de seguridad lógica, así como una pobre gestión de recursos de almacenamiento (Shacklett, 2021). De acuerdo con un estudio publicado recientemente por Palo Alto Networks (Unit 42, 2020) que consideró una población de más de un millón de dispositivos físicos inteligentes empresariales y de atención médica, se identificó que el 98% de todo el tráfico de red proveniente de estos dispositivos no está encriptado, de igual manera se identificó que el 57% de estos dispositivos presentan vulnerabilidades de seguridad que pueden ser aprovechadas por ciberdelincuentes para perpetrar ataques que pueden tener una gravedad media o inclusive alta. Afuera de los firewalls de las organizaciones podemos encontrar dispositivos físicos inteligentes críticos para el negocio, los cuales, sin lugar a duda, representan nuevos riesgos de seguridad informática, particularmente cuando posen capacidades de almacenamiento de datos o reconocimiento de imágenes mediante ejecución de algoritmos de aprendizaje automático. Estos dispositivos inteligentes, al igual que los equipos de red tradicionales, deben poder comunicarse de forma segura hacía un centro de datos, la nube u otros dispositivos de red, empleando técnicas como la encriptación de datos y autenticación de red como mecanismos de protección (Lee, 2020). Actualmente la mayoría de los principales proveedores de servicios de nube incluyen dentro de sus servicios, características de seguridad para la administración de dispositivos IoT dentro de sus plataformas, al igual que permiten cierta flexibilidad para que los equipos de TI propiedad de la organización puedan diseñar e implementar controles de seguridad personalizados a sus necesidades para garantizar que todos los dispositivos físicos inteligentes estén monitoreados y protegidos activamente.

Es importante considerar que los CIOs, CEOs y CFOs tienen un rol preponderante como parte de la evolución del gobierno de TI, donde tendrán que trabajar en conjunto en la implementación o mejora del proceso de abastecimientos de la organización con relación a la adquisición de dispositivos inteligentes, para definir procedimientos específicos para la evaluación detallada del proveedor o fabricante que abastecerá los dispositivos IoT ya que expertos en seguridad han identificado puertas traseras ocultas (backdoors) en algunos dispositivos que pueden usarse para enviar información de vuelta al fabricante (Privitera & Li, 2018), por lo que salvaguardar, asegurar y controlar este tipo de dispositivos es una tarea que inicia mucho antes de la propia operación.

De la misma manera en que observamos esta evolución en la forma en la que las organizaciones aprovechan el avance tecnológico para hacerse más fuertes y competitivas, es altamente recomendable, incluso imprescindible, que las estrategias, políticas y procedimientos de gobernanza y control deban evolucionar para satisfacer las necesidades de una nueva generación de dispositivos inteligentes con una visión holística de la organización y con la participación activa de la alta dirección.

¿Qué regulaciones se pueden incumplir debido a la falta de gobierno de dispositivos IoT?

La introducción de dispositivos capaces de reconocer patrones de comportamiento, reconocer imágenes o transaccionar con datos biométricos, ha representado un desafío para las organismos reguladores locales así como para organismos globales en busca de garantizar un uso apropiado de esta tecnología sin descuidar temas tan sensibles como el acceso y privacidad de los datos, o por otro lado asegurar que los dispositivos se alinean con los marcos de control de las organizaciones listadas en el mercado bursátil de Nueva York, las cuales por regulación deben emitir anualmente reportes de control interno en los que se incluye el comportamiento del gobierno sobre el ambiente tecnológico de una organización, considerando, desde luego, los dispositivos físicos inteligentes.

Las regulaciones actuales han centrado su atención principalmente en el cumplimiento de disposiciones que garanticen que la información que es transaccionada a través de los dispositivos físicos inteligentes no ponga en riesgo la privacidad de los datos personales de los usuarios; consideremos la situación actual de México con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES, 2010), de acuerdo con esta regulación es necesario otorgar un consentimiento explicito para que un tercero pueda almacenar, procesar o transferir datos personales de cualquier individuo, definiendo como datos personales todos aquellos que hacen identificable a una persona, por ejemplo, nombre o clave única de registro de población (CURP), por lo que el cuestionamiento es ¿Cómo un dispositivo IoT que procesa datos personales obtiene el consentimiento explícito para tratar estos datos?. La pregunta anterior es uno de los principales retos que se plantean los organismos reguladores, las empresas y los mismos usuarios, a menudo los avisos de privacidad no comunican claramente los riesgos del procesamiento de datos y la vinculación que los registros obtenidos pueden hacer hacía un individuo.

En un contexto internacional encontramos la Regulación General de Protección de Datos (GDPR por sus siglas en inglés) publicada en abril de 2016 por la Unión Europea (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance), 2016), la cual se ha convertido de manera paulatina en un estándar global o al menos una base para el desarrollo de reglamentos locales. Esta regulación ha definido principios de gobierno de TI relativos al procesamiento de datos y establece nuevos estándares para la protección de datos en dispositivos físicos inteligentes (Artículos 5 y 25) (Wachter, 2018).

La GDPR es un buen punto de partida para abordar discusiones más extensas y profundas sobre los límites de la privacidad de los datos que son capturados por los dispositivos físicos inteligentes y como éstos hacen identificable a un usuario, cliente, consumidor, proveedor, empleado, etcétera. De acuerdo con (Wachter, 2018) existen cuatro retos principales a ser considerados en el uso de dispositivos IoT, tanto a nivel doméstico-personal, así como a nivel empresarial, los cuales son: 1) Perfilamiento, inferencia y discriminación. 2) Control y transferencia de datos personales. 3) Consentimiento y 4) Trasparencia. Estos retos deben ser analizados en el contexto de los nuevos requerimientos de protección de datos introducidos por la GDPR.

Hasta el momento hemos repasado las implicaciones regulatorias que plantea el uso de dispositivos IoT con un enfoque mayor hacía la privacidad de los datos y como éstos son tratados. No obstante, la introducción de sistemas de información conectados con dispositivos físicos inteligentes para la toma de decisiones en la operación de una organización es un tema central en la agenda de la alta dirección, no solamente como un habilitador para mantener la operación del negocio sino más bien como un pilar para el desarrollo de una clara ventaja competitiva en el mercado. Bajo esta perspectiva encontramos también regulaciones que se deben acatar, desde un punto de vista financiero, principalmente para las organizaciones que cotizan sus acciones en los mercados de valores del mundo.

El escándalo de Eron Corporation mostró de manera contundente como la falta de un modelo de gobierno corporativo apropiado, incluido el gobierno de TI puede significar la debacle de una organización (Benston & Hartgraves, 2002). Este escándalo además de dejar una serie de lecciones aprendidas también legó legislaciones alrededor del mundo que ayudan a combatir prácticas fraudulentas en las organizaciones y que protejan los derechos de los inversionistas, de esta manera es como, particularmente para el mercado Estadunidense, encontramos la ley Sarbanes-Oxley (SOX) promulgada en Julio de 2002 (An Act to Protect Investors by Improving the Accuracy and Reliability of Corporate Disclosures Made Pursuant to the Securities Laws, and for Other Purposes., 2002), la cual,

sentó un precedente en el mercado bursátil al imponer requisitos más robustos y estrictos a los que deben estar sujetas las organizaciones que deseen capitalizarse mediante la comercialización de sus acciones en la bolsa de valores de Estados Unidos principalmente, sin embargo esta regulación aplicable solo en la geografía Norte americana se convirtió en la punta de lanza para que gobiernos de otros países adoptaran leyes similares, adecuadas a sus necesidades, que protegieran a los inversionistas de las bolsas de valores locales, tal es el caso de México o Japón.

La ley SOX como es comúnmente conocida en el mundo, es de carácter obligatorio aplicable a entidades basadas en Estados Unidos, basadas en otros países o subsidiarias significativas de empresas que comercializan sus acciones en la bolsa de valores de Nueva York, está regulación está centrada en la prevención de fraudes por parte de las empresas hacía sus accionistas tomando como pilares fundamentales para alcanzar este objetivo la aplicación de normas de contabilidad y la implementación de un modelo adecuado de gobierno de corporativo que incluya la definición de un marco de control interno para garantizar que existan mecanismos de control razonables que aseguran que las cifras reportadas en los estados financieros son verídicas. La ley SOX demanda que las organizaciones directamente cotizantes o subsidiarias significativas de un cotizante directo en la bolsa de valores de Nueva York presenten de manera periódica un informe detallado de la situación financiera de la organización así como una opinión del estado de su marco de control interno sobre los estados financieros, la cual debe ser emitida por un organismo tercero certificado y facultado para poder hacerlo, es en este punto en el que se formula la pregunta, ¿Son los dispositivos físicos inteligentes implementados en la operación de una organización relevantes para la elaboración de sus estados financieros?

En un contexto digitalizado como en el que nos encontramos, en el que observamos cada vez con mayor frecuencia y a mayor escala la interacción de dispositivos IoT en los procesos de negocio de una organización, definitivamente debemos considerar el impacto que éstos tienen en la recopilación, tratamiento y almacenamiento de datos que serán el insumo principal para el registro de las operaciones de la organización y que a la postre servirán para la elaboración de los estados financieros. De esta manera es de suma importancia que los CIOs, CEOs, y CFOs trabajen en conjunto para identificar que dispositivos físicos inteligentes son relevantes para el reporte financiero, que ciclos de negocio son los que mayormente usan dispositivos IoT para realizar sus operaciones, que cuentas contables se ven afectadas por los datos transaccionados por estos dispositivos, que información recolectada por estos dispositivos es utilizada en tiempo real para determinar el desempeño de un proceso o línea de producción, entre otros cuestionamientos que les permitirán realizar un análisis de riesgo apropiado que será la base para la extensión o implementación de un modelo de gobierno de TI, que diseñe mecanismos de control apropiados para asegurar que la apropiada operación, monitoreo y reporte del estado de los dispositivos físicos inteligentes en función de su relevancia a nivel reporte financiero. Por lo que con este entorno digital jugando un papel preponderante en el cumplimiento de estándares de auditoría y contabilidad, los elementos de TI y en especial los dispositivos IoT se convierten también en objetivos de regulación y evaluación periódica bajo la normatividad SOX (Mangalaraj et al., 2022).

Trabajo Futuro

Las conclusiones alcanzadas en esta investigación indican que mayor trabajo puede ser realizado para el desarrollo de un modelo de gobernanza optimizado para los dispositivos IoT, el cual pueda brindar a las organizaciones el conjunto de buenas prácticas y un marco de trabajo definido que pueda implementarse en sus ambientes tecnológicos que les permita contar con mecanismos razonables de aseguramiento de seguridad y privacidad de los datos capturados y procesados por estos dispositivos.

3. CONCLUSIONES

Las organizaciones y sus líderes se preocupan cada vez más por brindar una experiencia de cliente impulsada por la tecnología, lo que requiere una mayor sincronización entre todos los elementos del entorno tecnológico y por ende también en los dispositivos físicos inteligentes. Los dispositivos IoT requieren diferentes niveles de robustez en su manufactura, gestión y gobierno, ya que un mal funcionamiento, un servicio no disponible o un uso no autorizado de éstos puede desencadenar una serie de riesgos que pueden entorpecer el cumplimiento de los objetivos estratégicos y comerciales de la organización. La definición de un modelo de gobierno de TI integral que contemple una visión holística de la organización y que permee hacía los dispositivos IoT, que cada vez tienen más presencia en los entornos tecnológicos empresariales, es un tema de gran relevancia en la agenda de la alta dirección.

Por esta razón tanto CIOs como CEOs and CFOs deben asegurarse de que sus dispositivos físicos inteligentes sean capaces de cumplir con los estándares y regulaciones actuales que fomentan la reducción de incidentes que puedan derivar en consecuencias graves para las empresas. Es imprescindible contar con la colaboración de líderes a través de la organización y con especialistas de TI para garantizar que la cultura que rodea a los dispositivos IoT promueva la seguridad, la protección y la confidencialidad de los usuarios. Dada la importancia de los dispositivos inteligentes en los entornos tecnológicos organizacionales actuales, las áreas de TI cada vez están a cargo de un número mayor de estos dispositivos, por lo que el gobierno y gestión de éstos no es una tarea de una sola dirección más sin en cambio el involucramiento oportuno de la dirección ejecutiva y la dirección de finanzas es crucial para modelar un sistema de gobierno y control que dé respuesta a los riesgos inherentes que el uso de estos dispositivos introduce a la organización, son estas direcciones (CIO, CEO y CFO) quienes deben examinar las implicaciones tecnológicas, financieras y de operación que trae consigo la implementación cada vez mayor de tecnología física, así como mantener una cultura de evaluación constante del riesgo, ya que si bien son muchas las bondades que este tecnología trae para la organización, no se puede negar que también introducen un aumento en la exposición al riesgo, incluidos los potenciales daños a la reputación de la organización por un incumplimiento en el tratamiento de datos personales, o de la caída del precio de las acciones por la identificación de fallas o violaciones de seguridad derivadas de una mala gestión y control de estos dispositivos.

4. REFERENCIAS

An act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. (No. 204, 204). (2002). U.S. Government Printing Office. https://www.govinfo.gov/app/details/PLAW-107publ204

Brockmann, V., Stölzle, W., & Wiedemann, A. (2018). A CEO and CFO perspective on Internet of Things implementation in manufacturing firms. International Journal of Operations & Production Management, 38(1), 118-138.

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. International Journal of Information Management, 51, 101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008

Chanal, P. M., & Kakkasageri, M. S. (2020). Security and Privacy in IoT: A Survey. Wireless Personal Communications, 115(2), 1667–1693. https://doi.org/10.1007/s11277-020-07649-9

DOF - Diario Oficial de la Federación. (2010, July 5). https://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010#gsc.tab=0

ISACA. (2018, November 9). Store—COBIT 2019 Framework: Governance and Management Objectives | Print | English—ISACA Portal. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko5aEAC

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 119 OJ L (2016). http://data.europa.eu/eli/reg/2016/679/oj/eng

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), Article 9. https://doi.org/10.3390/fi12090157

Malik, P. K., Sharma, R., Singh, R., Gehlot, A., Satapathy, S. C., Alnumay, W. S., Pelusi, D., Ghosh, U., & Nayak, J. (2021). Industrial Internet of Things and its Applications in Industry 4.0: State of The Art. Computer Communications, 166, 125–139. https://doi.org/10.1016/j.comcom.2020.11.016

Manavalan, E., & Jayakrishna, K. (2019). A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. Computers & Industrial Engineering, 127, 925–953. https://doi.org/10.1016/j.cie.2018.11.030

Pivoto, D. G. S., de Almeida, L. F. F., da Rosa Righi, R., Rodrigues, J. J. P. C., Lugli, A. B., & Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. Journal of Manufacturing Systems, 58, 176–192. https://doi.org/10.1016/j.jmsy.2020.11.017

Privitera, D., & Li, L. (2018). Can IoT Devices Be Trusted? An Exploratory Study. Emergent Research Forum.

State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. (2020, November 19). IoT Analytics. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

Shokoohyar, S., Shokouhyar, S., & Zarrin, S. (2020). Analysing the impact of IT governance on the performance of project-based organisations. International Journal of Business and Systems Research, 14, 411. https://doi.org/10.1504/IJBSR.2020.10031085

Syd Ali, B. (2019). Traffic management for drones flying in the city. International Journal of Critical Infrastructure Protection, 26, 100310. https://doi.org/10.1016/j.ijcip.2019.100310

Tian, Y., Yuan, J., & Song, H. (2019). Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. Journal of Information Security and Applications, 48, 102354. https://doi.org/10.1016/j.jisa.2019.06.010

Unlocking the potential of the Internet of Things | McKinsey. (n.d.). Retrieved May 15, 2023, from https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Computer Law & Security Review, 34(3), 436–449. https://doi.org/10.1016/j.clsr.2018.02.002