AUDITORÍA A LOS CONTROLES UTILIZADOS EN LOS COBOTS, PARA EVITAR FRAUDES EN PROCESOS INDUSTRIALES

Ing. Hector Ancizar Benavides Vallejo[1]

Resumen

En el artículo se identifican las características de los cobots las cuales permiten el desarrollo de un trabajo colaborativo con humanos, ocasionando que los procesos industriales se realicen con eficiencia, altos estándares de calidad, oportunidad y reducción de costos. Por otra parte, se determinan las vulnerabilidades que impactan en los cobots con una severidad de riesgo alto, en el software y el hardware a través de ataques remotos y físicos, los cuales pueden manipular esta tecnología, causando desde el robo de información clasificada hasta daños en el recurso humano por lesiones. Por consiguiente se identifican y evalúan los controles existentes en los cobots, aplicando la metodología ISO 19011 apoyada por la gestión de riesgos (ISO 31000), obteniendo como resultado que los controles no son eficientes, ni apropiados para mitigar los riesgos, por lo tanto, se recomienda que se implementen auditorías de sistemas, como un control detectivo, las cuales deben ejecutarse periódicamente con el objetivo de evaluar el estado de los controles y a su vez analizar si es necesario implementar nuevos controles.

Palabras Claves (Cobots, Auditoría de sistemas, Controles, Fraudes, Malas prácticas)

Abstract

In the article, the characteristics of cobots are identified which allow the development of collaborative work with humans, causing industrial processes to be carried out with efficiency, high quality standards, opportunity and cost reduction. On the other hand, vulnerabilities that impact cobots with a high-risk severity, in software and hardware are determined through remote

[1] HECTOR ANCIZAR BENAVIDES VALLEJO, Ingeniero Electrónico, Especialista en Auditoría de Sistemas egresado de la Universidad Antonio Nariño, Correo: ancizar.benavides@gmail.com.

and physical attacks, which can manipulate this technology, causing from the theft of classified information to damage in the human resource for injuries. Therefore, the existing controls in the cobots are identified and evaluated, applying the ISO 19011 methodology supported by risk management (ISO 31000), obtaining as a result that the controls are not efficient, nor appropriate to mitigate risks, therefore, It is recommended that systems audits be implemented, such as a detective control, which should be carried out periodically in order to evaluate the state of the controls and in turn analyze whether it is necessary to implement new controls.

Key Words (Cobots, Systems Audit, Controls, Fraud, bad practices)

Introducción

Los robots industriales han estado en uso desde hace seis décadas, sus aplicaciones comunes incluyen la fabricación de automóviles, de productos electrónicos, el montaje de materiales, la manipulación de objetos, el movimiento y embalaje de materiales para su distribución. Sin embargo, en los últimos años, se ha observado un evidente aumento en el interés por los robots colaborativos (cobots), debido a la obtención de beneficios en precisión, calidad y productividad.

Por lo tanto, los cobots llegan para quedarse y seguir evolucionando; su importancia se puede señalar en el trabajo colaborativo con humanos, en donde uno de los factores con prioridad es la seguridad, aplicando los requisitos que especifica la ISO 10218 e ISO/TS 15066, con el objeto de lograr una cadena de producción eficaz, oportuna y con altos estándares de calidad.

No obstante, si esta tecnología va a recibir una amplia aceptación, uno de los desafíos clave es crear sistemas de gestión de riesgo que promuevan el desarrollo de la industria de la robótica y al mismo tiempo se mitiguen las amenazas por ataques cibernéticos (remotos y físicos).

En pocas palabras, los empresarios no adquirirán cobots a menos que crean que son seguros o cuente con controles que mitigue dichas amenazas. En consecuencia, los fabricantes deberán establecer sus propias prácticas para diseñar productos seguros y minimizar su responsabilidad. Usualmente se considera que la responsabilidad del producto cae directamente a los fabricantes o a las compañías que piensan ingresar a la industria de la robótica. En efecto, los fabricantes realmente deben investigar y analizar cómo mitigar los riesgos de fraude por malas prácticas ya que según empresas prestigiosas que se dedican a analizar e investigar la seguridad en los cobots, detectaron tres factores claves de riesgo como: la seguridad del recurso humano, la integridad de los datos que procesa un cobot y la precisión de la producción en cadena.

Por lo tanto, existe la necesidad de la auditoría de sistemas con el fin de evaluar los controles que utilizan los cobots, para mitigar los fraudes en procesos industriales oportunamente, en consecuencia, la pregunta a resolver en el desarrollo de este artículo es ¿Cómo identificar y evaluar los diferentes controles, que evitan fraudes y malas prácticas en los cobots en la producción industrial?

Este artículo está enfocado en la realización de una investigación explicativa en donde se busca exponer la ocurrencia de ciertos eventos y en qué circunstancias se generan. Como primer paso se recolecta información de los procedimientos y funciones que cumplen los cobots en los procesos industriales, para luego identificar y analizar los fraudes por malas prácticas, llegando finamente a la evaluación de los controles a través del análisis del sistema de gestión de riesgos.

Objetivos

Objetivo general

Evaluar por medio de la auditoría de sistemas los diferentes controles que existen en los cobots de procesos industriales automatizados, para evitar fraudes y malas prácticas.

Objetivos específicos

- Identificar las funciones que cumplen los cobots, en los procesos industriales.
- Determinar los fraudes que se podrían presentar en el uso de los cobots, en procesos industriales automatizados.
- Diagnosticar a través del sistema de gestión de riesgos, los controles de los cobots utilizados en los procesos industriales automatizados.

Metodología

La elaboración del articulo está enfocada en el método inductivo y el tipo de estudio que se utilizara es explicativo. Para la investigación se hace uso de la revisión documental, consultas en internet, consultas en bases de datos electrónicas como www.academia.edus, www.cielo.org, la IEEE, libros de robótica colaborativa, revistas, videos y cualquier material consultado en páginas electrónicas que haga referencia con el tema de auditoría a los controles utilizados en los cobots, para evitar fraudes en procesos industriales.

Marco Contextual

Desde finales de la década de 1990, las tendencias están cambiando, en gran parte debido a las obvias deficiencias de la automatización para cumplir con los costos y expectativas de flexibilidad. En lugar de tener grandes células robotizadas estáticas, se está optando, por la tendencia a los robots colaborativos (cobots), los cuales son unidades industriales flexibles, con una gran capacidad de cambio en los procesos al ser compartidos con humanos en un trabajo colaborativo. En los últimos años la tecnología de los robots colaborativos (cobots), se ha convertido en el detonador del crecimiento de las industrias, al automatizar sus procesos, permitiendo la expansión de las grandes cadenas de producción en la mayoría de los países y al

mismo tiempo entrando a un mundo globalizado, por lo tanto, los costos de fabricación de los productos tienden a bajar (Fast-Berglund, Palmkvist, Nyqvist, Ekered, & Åkerman, 2016).

Teniendo en cuenta lo antes mencionado y como ya se conoce que los robots colaborativos están cada vez más presentes en los entornos industriales, incluso en sectores críticos (farmacéutica, medicina), a menudo están conectados al mundo exterior a través de internet, convirtiéndolos en un blanco fácil para ataques de hackers informáticos, lo que puede ser causa de riesgos de ciberseguridad asociados con los robots colaborativos (Kovacs, 2017).

Según Kovacs (2017), durante su análisis de vulnerabilidades, los expertos descubrieron que un número creciente de robots colaborativos industriales, incluyen funciones de acceso remoto, diseñadas para monitoreo y mantenimiento como se puede observar en la *figura 1*.

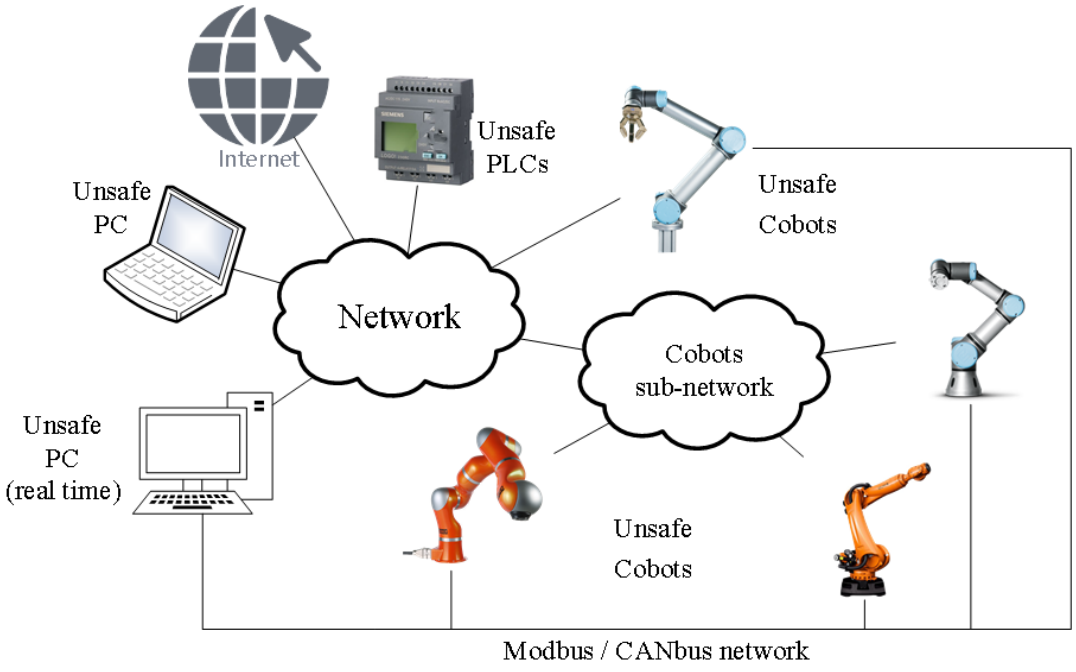


Figura 1. Sistema distribuido robótico.
Fuente. (Vicentini, y otros, 2014).

Si bien estas características pueden ser útiles para los operadores, también pueden presentar serios riesgos de seguridad. En mucho de los casos los escaneos de internet realizados

con los servicios Shodan, Censys y ZoomEye[2] mostraron que algunos robots están expuestos a internet a través de sus servidores FTP[3]. Los expertos identificaron más de dos docenas de cobots expuestos en Europa, Estados Unidos, Asia y Australia. Ahora bien, estas vulnerabilidades detectadas son fuentes de riesgo, que aprovechadas por personas mal intencionadas pueden llegar a causar fraudes y malas prácticas en los cobots, por ende, es importante que a través de la auditoría de sistemas y la gestión de riesgos se evalúen si los controles de los robots colaborativos son efectivos y funcionales.

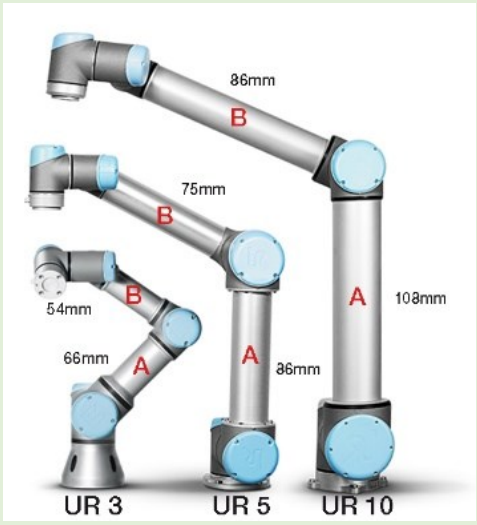
Antecedentes

¿Qué son los cobots?, para contestar esta pregunta es importante conocer la historia de cómo inicio la construcción del primer robot industrial el cual por razones de seguridad tenía que permanecer dentro de jaulas para proteger a los humanos que trabajaban cerca de él, hasta la evolución y concepción de los robots colaborativos los cuales ya son seguros y no necesitan jaulas para trabajar colaborativamente con humanos *ver tabla 1*.

Tabla 1. Historia de los cobots, como inicio todo.

Año	Descripción
1920	Se escucha por primera vez la palabra robot en una obra de ciencia ficción denomina *Rossum's Universal Robots*, la cual fue inventada por el escritor checo Karel Capek.
1954	Se construye el primer brazo robot industrial, llamado dispositivo de transferencia de articulo programado, el cual fue patentado por George Devol, quien luego se asocia con Joseph Engelberger y es lanzado al mercado en 1959 e instalándose la primera unidad en General Motors.
1960-2000	Los robots industriales aún permanecen enjaulados debido a la inseguridad latente para con los humanos, y al mismo tiempo estas tecnologías necesitaban empresarios que realizaran importantes inversiones y personal con experiencia en programación, por lo tanto, los robots industriales se empezaron a generalizar en la industria automotriz y otros sectores de fabricación de productos.
2001-2005	Un equipo de investigación de la universidad del Sur de Dinamarca, compara y analiza las soluciones de automatización existentes con las necesidades del mercado, descubriendo una oportunidad para reinventar el robot industrial.
2005	Es fundada la empresa Universal Robots, pionera en la robótica industrial, esta empresa la fundan 3 miembros del equipo investigador de la Universidad del Sur de Dinamarca, y se enfocan en desarrollar un robot rápido, colaborativo y fácil de usar, con un rápido ROI (Return on Investment).

[2] Son motores de búsqueda que permiten detectar las vulnerabilidades de los dispositivos que se conectan a internet.
[3] Protocolo de transferencia de archivos, permite la comunicación bidireccional entre equipos remotos.

2008	Se lanza al mercado el primer cobot del mundo, llamado UR5 *ver figura 2*, fabricado por la empresa Universal Robots, este robot colaborativo es capaz de operar de manera segura junto a las personas.  *Figura 2. Primer cobot fabricado en el mundo, modelo UR5.* *Fuente. (Univelsal-Robots, 2018)*
2012	Se lanza al mercado el cobot UR10 *ver figura 3*, con mejoras en el alcance del brazo y mayor carga.  *Figura 3. Robots colaborativos modelos UR3, UR5, UR10.* *Fuente. (Univelsal-Robots, 2018)*
2012-2016	Collaborative Robotics, es reconocida como una nueva clase viable de robots; por lo tanto, los fabricantes de robots más grandes como Startups y las más pequeñas como Rethink Robotics, comienzan a desarrollar cobots y lanzan estos productos al mercado.
2014	Una organización alemana que trabaja validando la seguridad de los productos, certifica el sistema de seguridad de tercera generación de los robots colaborativos UR
2015	Universal Robots lanza al mercado el cobot UR3 *ver figura 3*, el cual es el primer robot colaborativo de mesa del mundo.
2016	Llega la tan espera normatividad, la ISO/TS 15066 la cual contiene guías para garantizar la seguridad de los trabajadores humanos en sistemas robóticos colaborativos.

Fuente. Elaboración propia con datos de (Univelsal-Robots, 2018)

Teniendo en cuenta la historia de los robots colaborativos se pueden describir como máquinas que permiten automatizar los procesos industriales; estos robots son programados con inteligencia artificial, por lo tanto, pueden realizar una serie de acciones complejas de forma

autónoma, interactuando de manera segura en el trabajo colaborativo con los humanos como se observa en la *figura 4*.

Figura 4. Robot-Humano, trabajo colaborativo.
Fuente. (Kuka, 2018)

A continuación, los factores más importantes que componen un cobot son: se conforman de hardware y software, se conectan al exterior a través de la tecnología IoT, interactúan con el mundo físico a través de sensores y actuadores, son programables, suelen ser autónomos, cuenta con algoritmos de inteligencia artificial permitiéndoles ejecutar actividades complejas (Chinecherem, Kenneth, & Hycient, 2017).

Cabe destacar que, en la industria manufacturera, los empresarios que buscan hacer una compra de robots a menudo tienen algunas ideas erróneas sobre la tecnología que desean implementar. Por estas razones, a continuación, se presenta una clara diferencia entre los robots industriales tradicionales y los cobots *ver tabla 2.*

Tabla 2. Cobos vs Robots industriales tradicionales.

Cobots	**Robots industriales tradicionales**
Instalaciones diferentes, sin espacio adicional requerido.	Instalación fija, grandes requisitos de seguridad.
Con interacción frecuente de empleados humanos.	Sin interacción de empleados humanos.
Desarrollan múltiples tareas.	Única tarea o proceso.

Son programables por el operario de manera sencilla, rápida, y tienen la capacidad de aprender en el trabajo.	Programación con costo alto y depende de su proveedor, por lo tanto, es necesario que un ingeniero escriba o modifique el código para implementar cambios en el proceso.
Retorno de inversión inferior a un año.	Alta inversión, retorno en varios años.
Trabajo colaborativo con empleados humanos.	Reemplaza a los empleados humanos.
Apoyan a los empleados humanos con trabajos peligrosos, extenuantes, o repetitivos para que puedan realizarlos por sí mismos, creando un lugar de trabajo más eficiente y seguro, sin tener que eliminar o modificar procedimientos del proceso de producción.	Automatizan el proceso de fabricación casi por completo, sin ayuda humana en la planta de fabricación.
No están diseñados para la fabricación pesada, lo que permite el trabajo en equipo con humanos.	Pueden manejar material pesado y de grandes dimensiones, como los utilizados en la fabricación de automóviles y por ende deben estar enjaulados, no hay humanos interactuando.

Fuente. Elaboración propia con datos de (Müller-Abdelrazeq, Schönefeld, Haberstroh, & Hees, 2019)

Cuando se habla de cobots debe tenerse en cuenta los siguientes conceptos: Ciberataques, es cualquier tipo de maniobra ofensiva que se dirige a sistemas, infraestructuras, redes o dispositivos informáticos personales. Un atacante es una persona o proceso que intenta acceder a datos, funciones u otras áreas restringidas del sistema sin autorización, con intención maliciosa (Hussain, y otros, 2017).

Modbus, se denomina como protocolo de comunicación industrial, la transmisión de datos se realiza en serie, puede ser síncrona o asíncrona, es muy común utilizarlo en la comunicación entre dispositivos electrónicos, en este caso entre robots colaborativos; este protocolo es muy vulnerable a los ataques (espionaje industrial e infiltraciones) (Tanenbaum, 2012).

Acceso y control remoto, permite a los proveedores de los cobots, prestar el servicio de mantenimiento y soporte de TI a través de redes privadas como las VPN, accediendo a los equipos de manera remota sin esfuerzo. Las herramientas de acceso remoto en línea deben ser compatibles con cortafuegos y estar completamente protegidos a través de SSL para establecer conexiones remotas rápidas y seguras; este tipo de accesos sin un buen control de seguridad se puede convertir en una puerta trasera por donde los hackers pueden atacar.

Fraudes, es la manipulación, falsificación o alteración de registros de programación de un cobot, con el objeto de adquirir beneficios económicos; estos fraudes pueden ser ejecutados por personal interno de la empresa con vínculo laboral o personal externo sin vínculo laboral.

Riesgo, “consististe en eventos relacionados con TI que podrían impactar potencialmente en el negocio” (ISACA, 2018).

Vulnerabilidad, se define como las características que hacen susceptibles a los cobots ante efectos dañinos de una amenaza.

Normatividad

Cuando se construyen maquinas que van a interactuar en un trabajo colaborativo, con trabajadores humanos en la producción industrial, es importante que los diseños, la fabricación e implementación de los cobots se rijan a unas normas de seguridad las cuales son: ISO 12100: 2010 contiene los principios y la metodología para lograr la seguridad en el diseño de maquinaria. Entre estas especificaciones se encuentra la evaluación de riesgos y la evaluación del tratamiento para la reducción del riesgo inherente (ISO-12100, 2010); la ISO 13849-1: 2015, proporciona requisitos de seguridad y orientación sobre los principios para el diseño e integración de safety-related parts of control systems (SRP/CS), incluido el diseño de software (ISO-13849-1, 2015); la ISO 10218-1: 2011, especifica requisitos y lineamientos para el diseño seguro e inherente a medidas de protección y/o información para el uso de robots Industriales (ISO-10218-1, 2011); la ISO 10218-2: 2011, suministra requisitos para eliminar o reducir adecuadamente los riesgos asociados en la integración de robots industriales (ISO-10218-2, 2011); la ISO / TS 15066: 2016 especifica los requisitos de seguridad para los sistemas de robots industriales colaborativos y el entorno de trabajo (ISO/TS-15066, 2016); la IEC 61508: 2010, permite considerar aquellos aspectos cuando se utilizan sistemas electrónicos, eléctricos y

electrónicos programables (E / E / PES) para llevar a cabo funciones de seguridad (IEC-61508, 2010).

Ejecución de una auditoría de sistemas con un enfoque basado en análisis de riesgos

Para el desarrollo del artículo, se hace uso de los lineamientos proporcionados por la Norma ISO 19011:2018, la cual contiene las fases y criterios para realizar una auditoría de sistemas eficiente y practica permitiendo analizar y evaluar los controles que tienen los cobots, a través de la planeación, ejecución y el dictamen. Por otra parte, el sistema de gestión de riesgos (ISO 31000:2018), complementa la auditoría de sistemas al permitir identificar los escenarios, las amenazas, su severidad y los controles existentes, observar la *figura 5*.

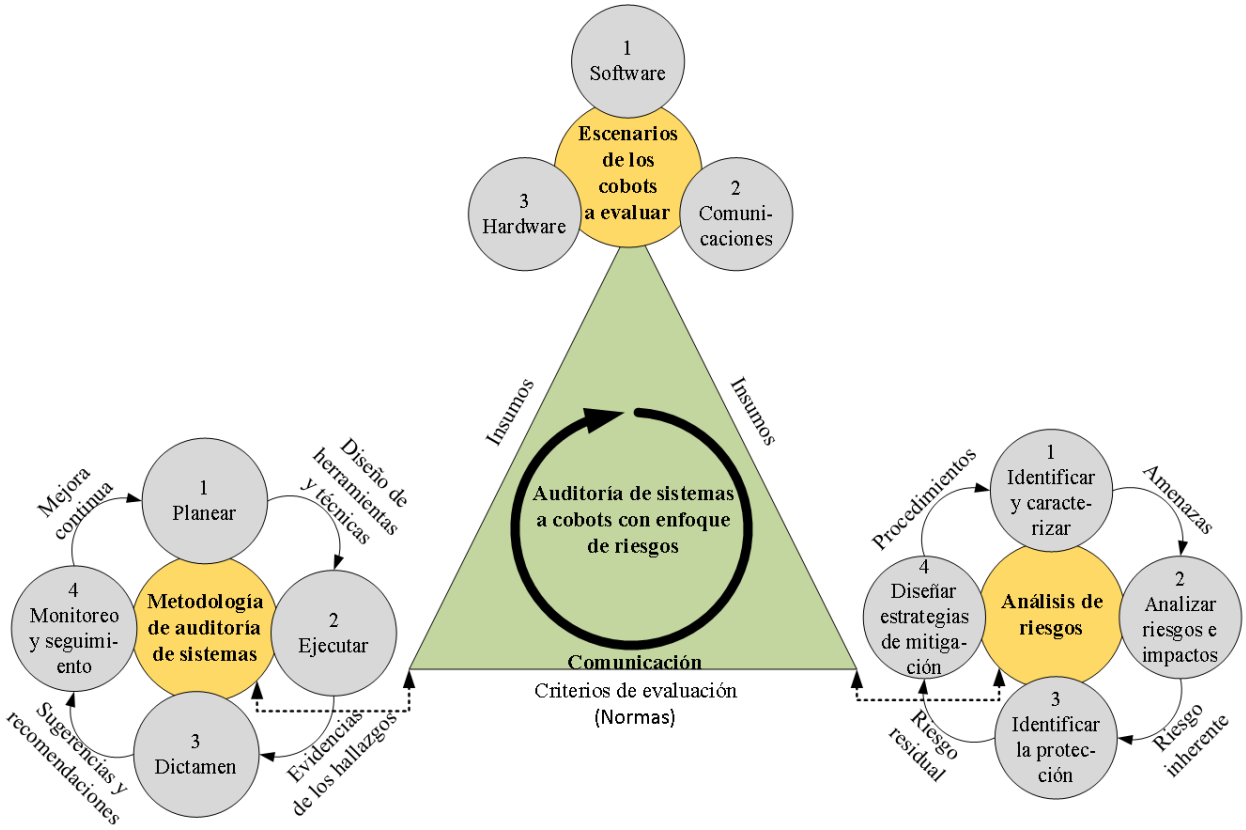


Figura 5. Auditoria de sistemas a cobots con enfoque de riesgos.
Fuente. Elaboración propia con datos de (ISO 19011:2018), (ISO 31000:2018).

Resultados

Los cobots al ser máquinas de trabajo colaborativo con personal humano, cada vez se incorporan en más aplicaciones industriales, como las siguientes:

Control de calidad automatizado, se realiza a través de un robot colaborativo el cual tiene instalado una cámara, permitiendo realizar mediciones en 3D y otras pruebas no destructivas para garantizar la calidad de los productos examinados, y así detectar de manera eficiente y fácil las piezas defectuosas antes de su empaquetado o envío, su aplicación se encuentra implementada en la industria automotriz, procesamiento de alimentos, farmacéutica, entre otros.

Líneas de montaje automatizadas, permite reducir los tiempos, sin afectar la calidad del producto; ejecuta procesos de ensamblaje precisos y repetitivos, como atornillar, encajar piezas e insertar, y al mismo tiempo se reducen las lesiones en los trabajadores humanos por repetitividad en el lugar de trabajo.

Supervisión de maquinaria, los sistemas de control automáticos pueden ser repetitivos y molestos para las personas, lo cual está asociado a riesgos laborales por esfuerzo repetitivo, por equivocación o por trabajar cerca de maquinaria pesada. En la actualidad, estos riesgos pueden eliminarse usando un robot colaborativo ya que estos pueden supervisar de forma constante y continua el funcionamiento de otras máquinas, mejorando los procesos y evitando los riesgos laborales.

Pruebas y análisis de laboratorio, los cobots pueden ser instalados en espacios reducidos, de tal manera que realicen procesos para tomar muestras de manera precisa, para luego distribuirlas, en los módulos de análisis correspondiente, garantizando condiciones de trabajo óptimas para el estudio y análisis en laboratorios, sin necesidad de una supervisión humana.

Lijado y pulido, garantiza la uniformidad de procesos de pulido y abrillantado, incluso en superficies irregulares y curvas, la posición y la fuerza se pueden ajustar o configurar en el software para un resultado óptimo, esta aplicación tiene mucha demanda en la industria automotriz.

Como se pude observar en las aplicaciones mencionadas, los impactos por ataques remotos o físicos son graves, ya que pueden afectar a la organización en imagen, pérdidas financieras, perdida de información clasificada, y recursos humanos que trabaje colaborativamente con los cobots; por tal motivo cabe destacar la importancia de la auditoría de sistemas con enfoque de riesgos, porque permite identificar las fuentes, las amenazas, su severidad con el objetivo de evaluar el tratamiento y ver si este es efectivo y funcional.

Teniendo en cuenta la investigación y la metodología de auditoría con enfoque de riesgos, se detectó que los cobots son vulnerables a ataques remotos o físicos; los ataques remotos pueden ser ejecutados a través de la red fija de internet o la red móvil GPRS. Por lo tanto, estas vulnerabilidades se deben controlar y mitigar ya que los cobots de la cuarta generación necesitan la conexión de internet para la ejecución y actualización de actividades en los procesos industriales; no obstante los ataques físicos son más peligrosos que los ataques de red, este tipo de ataques pueden ser ejecutados por los operados de los cobots, ya que ellos cuentan con información privilegiada, la cual utilizan en las interfaces para programarlos de manera manual; otro tipo de acceso en el ataque fisco son las interfaces de entrada y salida que tiene el controlador de los cobots (RJ-45, CANbus, Modbus, Usb). Por lo general los atacantes realizan ingeniería inversa al software, el cual fácilmente lo pueden encontrar en la página web del fabricante y así descubren las vulnerabilidades que este tiene.

Teniendo en cuenta los dos tipos de infiltraciones que puede realizar el atacante y el análisis que se realiza a través de la auditoria de sistemas con enfoque de riesgos, se encontró los siguientes fraudes que impactan significativamente a los cobots y por ende a la organización, se debe tener en cuenta que los fraudes se ocasionan por las vulnerabilidades que detectan los atacantes al hacer reingeniería en los escenarios de software y hardware ver *tabla 4*.

Tabla 3. Identificación de fraudes en los robots colaborativos.

Escenarios	Fraudes	Descripción o causa	Impacto
Software	-	• Para el escenario del software los fraudes se ejecutan remotamente a través de la infiltración del software (panel de control), el cual se utiliza como medio de comunicación entre el usuario y el cobot.	-
	Robo de información clasificada.	• Causa: espionaje industrial, extracción de información vital de la organización, con el objeto de venderla a la competencia o hacer uso ilegal de ella.	• Financiero • Pérdida de tiempo
	Alteración de la información.	• Modificando los parámetros lógicos de trabajo del robot colaborativo causando: Reportes erróneos de producción, por ejemplo, el cobot fabrica 200 unidades de un producto, pero como fue alterado solo reporta 100 unidades.	• Financiero • Pérdida de tiempo
	Uso de un esquema de ransomware	• Restringiendo el ingreso al sistema del cobot, modificando las credenciales de validación del usuario, causando: la extorción a la organización a cambio de la liberación del equipo. Se debe tener en cuenta que este tipo de ataque requiere de la ingeniería social para obtener contraseñas.	• Financiero • Pérdida de tiempo
	Alteración de la programación lógica del cobot.	• Modificando los parámetros lógicos de trabajo del robot colaborativo causando: movimientos no coordinados y por ende daño del producto o mal funcionamiento del mismo. • Alterando los estados (on/off) del cobot, generando un espacio de trabajo inseguro para el trabajador humano sin que este se percate de la adulteración, causando: lesiones al trabajador y daño físico al mismo robot.	• Financiero • Imagen • Seguridad laboral

Hardware	-	• Para el escenario del hardware los fraudes se ejecutan a través de la infiltración física del controlador del cobot, por medio de un funcionario de la empresa. El funcionario ubica un transceptor GPRS en las líneas de comunicación de entrada y salida (CANbus, Modbus) de datos tipo serial, causando el espionaje por un atacante, de los datos que se transmiten bidireccionalmente, entre el software y el hardware. Una vez obtenido los datos, se realiza reingeniería para decodificar y obtener los comandos de validación y parámetros de configuración del robot, el último paso es construir un software réplica del original, a partir de este paso inicia la infiltración remota.	-
	Robo de información clasificada.	• Causa: espionaje industrial, extracción de información vital de la organización, con el objeto de venderla a la competencia o hacer uso ilegal de ella.	• Financiero • Pérdida de tiempo
	Alteración de la información.	• Modificando los parámetros lógicos de trabajo del robot colaborativo causando: Reportes erróneos de producción, por ejemplo, el cobot fabrica 200 unidades de un producto, pero como fue alterado solo reporta 100 unidades.	• Financiero • Pérdida de tiempo
	Alteración de la programación lógica del cobot.	• Modificando los parámetros lógicos de trabajo del robot colaborativo causando: movimientos no coordinados y por ende daño del producto o mal funcionamiento del mismo. • Alterando los estados (on/off) del cobot, generando un espacio de trabajo inseguro para el trabajador humano sin que este se percate de la adulteración, causando: lesiones al trabajador y daño físico al mismo robot.	• Financiero • Imagen • Seguridad laboral

Fuente. Elaboración propia

Teniendo en cuenta la *tabla 4,* se puede señalar que este tipo de sistemas colaborativos, cuando son atacados pueden ser muy peligrosos desde el punto de vista, como amenaza para la vida humana (seguridad laboral) hasta las afectaciones financieras, de imagen y de tiempo, en una organización. Ahora imagine las consecuencias, si se ejecutara un ataque en una industria china, en donde el número de robots colaborativos superan las 50 unidades.

En la investigación se identificó cuatro controles, a los cuales se les realizará la evaluación de efectividad y funcionalidad. Para evaluar los controles se utilizarán los siguientes criterios establecidos en la *tabla 5* y *tabla 6*.

Tabla 4. Criterios de evaluación de los controles

Puntaje	Criterio	Calificación individual	
15	Documentación	Si	15
		Parcialmente	7
		No	0
10	Aplicación	Siempre	10
		Aleatoria	5
50	Efectividad del control	El control es efectivo y tiene evidencia	50
		El control requiere mejorar	25
		El control no es efectivo	0
15	Grado de automatización	Automático	15
		Mixto	7
		Manual	5
10	Tipo de control	Preventivo	10
		Detectivo	8
		correctivo	3

Fuente. Elaboración propia

Tabla 5. Efectividad de los controles.

Efectividad del control	
Apropiada	81-100
Mejorable	61-80
Insuficiente	41-60
Deficiente	21-40
Muy deficiente	0-20

Fuente. Elaboración propia.

Tenido en cuenta la *tabla 4,* para mitigar los riesgos de robo de información clasificada, alteración de la información, uso de un esquema de ransomware, y alteración de la programación lógica del cobot, se identificó los siguientes controles pertenecientes a los escenarios de software y hardware. Por consiguiente, en la *tabla 7*, se relacionan los controles pertenecientes al escenario software, los cuales se someterán a una evaluación de funcionalidad y efectividad.

Tabla 6. Identificación y evaluación de controles escenario software

1. Control	Protocolo de seguridad de autenticación propietario
Descripción	Este control permite encriptar las credenciales de autentificación, con el objetivo de que el atacante no pueda ver la verdadera contraseña
Tipo	Preventivo
Efectividad	Mejorable, por lo tanto, la severidad del riesgo inherente es mitigada con dificultad y reducido a riesgo residual bajo.

Prueba	Se descargo un software demo desde la página de un fabricante de cobots, y se realizó el ingreso de contraseñas aleatorias las cuales no existen; el software no permitió el ingreso, mostrando una alerta de autenticación errada, se puede aludir que el aplicativo si cumple con la función de validación y encriptación correcta, se verifica la base de datos para ver una contraseña existente, pero se encuentra encriptada.
Recomendación	Se recomienda optimizar el control utilizando el algoritmo de encriptación sha1, para las credenciales de autenticación ya que según otras investigaciones la seguridad del protocolo propietario es muy débil.
2. Control	Actualización periódica de software
Descripción	Permite mitigar las vulnerabilidades corrigiendo errores de código o seguridad.
Tipo	Detectivo
Efectividad	Insuficiente, por lo tanto, la severidad del riesgo inherente es mitigada con dificultad reduciéndose a riesgo residual moderado.
Prueba	Se descargo un software demo desde la página de un fabricante de cobots, el cual tiene como fecha de última actualización agosto de 2019, esto indica que el software no está a la vanguardia de los ataques.
Recomendación	Es necesario optimizar el control o estudiar la posibilidad de cambiarlo; Como los fabricantes de cobots no lanzan actualizaciones en periodos cortos, es recomendable utilizar paquetes de seguridad confiables (software antimalware, firewall), permitiendo identificar amenazas o conductas sospechosas provenientes de los ciberataques, los cuales, si están a la vanguardia de las nuevas tecnologías, se debe tener en cuenta la importancia de contar con ambas capas de protección.

Fuente. Elaboración propia.

Teniendo en cuenta los resultados de la *tabla 7*, se sugiere implementar el control de la *tabla 8*.

Tabla 7. Recomendación de control

Control	Backups periódicos de datos
Descripción	Permite tener un punto de recuperación de los datos confidenciales de la organización.
Tipo	Preventivo
Efectividad	Apropiado, por lo tanto, la severidad del riesgo inherente es reducido a riesgo residual.
Prueba	Se realiza verificación de los scripts creados para las copias de seguridad automáticas, existen casos en donde se tiene que hacer de manera manual, pero se evidencia que la información se está resguardando, este proceso queda registrado en una bitácora.
Recomendación	Teniendo en cuenta que el control es apropiado, tratar de que el proceso sea de manera automática y no mixta.

Fuente. Elaboración propia

Una vez evaluados los controles del escenario software, procedemos con la evaluación de funcionalidad y efectividad de los controles pertenecientes al escenario hardware, ver *tabla 9*.

Tabla 8. Identificación y evaluación de controles escenario hardware

1. Control	NX Bit (also known as Data Execution Prevention or DEP)
Descripción	La función de Prevención de ejecución de datos (DEP), también conocida como No execute (NX), evita que una aplicación o servicio ejecute código malicioso en una región de memoria no ejecutable, previniendo ciertos tipos de ataques por desbordamiento de búfer en la memoria.
Tipo	Preventivo
Efectividad	Mejorable, por lo tanto, la severidad del riesgo inherente es reducido a riesgo residual bajo con dificultad.

Prueba	Se realiza una simulación siguiendo los parámetros del fabricante a través de una aplicación hyperterminal en este caso llamada Hércules. Se procede a realizar una conexión con el socket del servidor del robot colaborativo, una vez se genera el enlace; el servidor contesta conected: universal robotics dashboard server, esta conexión se realiza usando la IP del cobot y el puerto de comunicación nada más. Logrando manipular el robot con los comandos que el mismo fabricante entrega en la página web; por lo tanto, en cierta manera la vulnerabilidad es muy alta ya que no exige credenciales de autenticación.
Recomendación	Si la conexión remota por socket no va a cumplir con los mínimos protocolos de seguridad, como son las credenciales de autenticación, no es muy recomendable activar este servicio en los robots colaborativos.
2. Control	Algoritmo CRC (STM-32)
Descripción	Este tipo de algoritmo denominado suma de verificación, es muy utilizado en la transmisión de datos Modbus. El CRC prácticamente lo que hace es codificar la información enviada la cual una vez llaga a su destino se decodifica para comprobar que el CRC es idéntico al del receptor, si es así significa que la información esta correcta, en este caso se pretende que, al utilizar el CRC, el atacante no pueda ver la información que se está enviando.
Tipo	Preventivo
Efectividad	Insuficiente, por lo tanto, la severidad del riesgo inherente es reducido a riesgo residual moderado con dificultad.
Prueba	En este caso se busca en internet una página web que ofrece, el servicio de calculadoras de CRC online y se realiza la prueba de ingresar datos codificados los cuales se decodifica con facilidad. También se debe tener en cuenta que en internet se encuentran códigos para codificar y decodificar datos con CRC, estos códigos se los ejecuta en java, puede ser en eclipse o NetBeans.
Recomendación	Este control es muy bueno para verificar que la información llega correcta a su destino mas no evita infiltración y robo de información. Para evitar que los atacantes se infiltren a través de los periféricos del hardware, es necesario que se creen políticas de seguridad en donde se restrinja la manipulación e ingreso del personal, a los periféricos del controlador del cobot o en su defecto tratar de deshabilitar los periféricos sin uso.

Fuente. Elaboración propia

En resumen, la severidad de los riesgos identificados en la *tabla 4* es alta y los controles identificados en las *tablas 7 y 9*, una vez evaluados, no tuvieron resultados muy eficientes y apropiados, esto debido a que son tecnologías emergentes. Por lo antes mencionado, a continuación se recomienda algunos controles: implementar en el software de los cobots el cambio obligatorio de contraseñas periódicamente, con el objetivo de endurecer la seguridad y mitigar los riesgos de infiltración; capacitar a los usuarios y/o empleados para que no sean víctimas de ingeniería social o malware, con el objeto de mitigar los riesgos de infiltración; activar y/o implementar el bloqueo de cuentas de accesos, en el caso de que se detecte más de tres intentos de ingreso debe bloquearse el perfil de usuario; realizar backups periódicas del firmware, esto con el fin de que, si un cobot está infectado por un código malicioso, contar con una copia de respaldo de manera oportuna; configurar y/o implementar las actualizaciones

periódicas de firmware, estas actualizaciones permiten corregir errores de programación tanto en la operación como en la seguridad, mitigando las infiltraciones al hardware; crear políticas y/o instructivos de seguridad para controlar el uso de las interfaces de entrada y salida de datos a través de CANbus y Modbus, objetivo mitigar el riesgo de infiltraciones de hardware a través de transceptores GPRS ubicados por funcionarios de la misma empresa.

Cabe destacar que a los controles existentes y a los que se implementarán se les realizarán monitoreos a través de auditorías de seguimiento, las cuales se deben ejecutar periódicamente de acuerdo a la necesidad del control; en el seguimiento se revisará el proceso de cobots y se analizará los cambios que ha tenido, se verificara que los controles que se evaluaron sigan operando, se utilizarán técnicas y herramientas como: inspección, comparación, revisión documental, listas de chequeo y cuestionarios, para evaluar la efectividad de los controles existentes y de los controles por implementar.

Conclusiones

Las características de los cobots como: multitarea, inteligencia artificial, fácil programación de actividades y estándares de seguridad laboral, permiten el desarrollo de un trabajo colaborativo con humanos, ocasionando que los procesos industriales se realicen con eficiencia, altos estándares de calidad, oportunidad y reducción de costos.

Las vulnerabilidades que impactan en los cobots con una severidad de riesgo alto, se producen en el software y el hardware a través de ataques remotos y físicos, los cuales pueden manipular esta tecnología, causando desde el robo de información clasificada hasta daños en el recurso humano por lesiones. Por ende, es necesario la implementación de mecanismos que aseguren la confidencialidad e integridad de los datos.

Los controles existentes en los cobots, una vez evaluados con la metodología ISO 19011 y apoyada por la gestión de riesgos (ISO 31000), dieron como resultado que no son eficientes, ni apropiados para mitigar los riesgos inherentes (robo de información clasificada, uso de un esquema de ransomware, alteración de la programación lógica del cobot), por lo tanto, se recomienda que se implementen auditorías de sistemas, como un control detectivo, las cuales deben ejecutarse periódicamente con el objetivo de evaluar el estado de los controles y a su vez analizar si es necesario implementar nuevos controles.

Referencias

Müller-Abdelrazeq, S., Schönefeld, K., Haberstroh, M., & Hees, F. (2019). Interacting with Collaborative Robots—A Study on Attitudes and Acceptance in Industrial Contexts. *Oliver Korn*, 101-117.

Apa, L. (22 de 08 de 2017). *Ioactive*. Obtenido de Ioactive: https://ioactive.com/exploiting-industrial-collaborative-robots/

Chinecherem, O. O., Kenneth, N. C., & Hycient, I. (2017). Robotics and artificial Intelligence: differences and similarities. *International journal of computer science and information security*, 26-28.

Fast-Berglund, Å., Palmkvist, F., Nyqvist, P., Ekered, S., & Åkerman, M. (2016). Evaluating cobots for final assembly. *Elsevier B.V*, 175-180.

Hussain, J., Memon, S., Mehmood , S., Usman, M., Ali Khan, R., Abbasi, S., . . . Hussain, Z. (2017). A user friendly security framework for the protectionof confidential information. *International Journal of Computer Science and Network Security*, 2015-223.

IEC-61508. (2010). *Functional safety of electrical/electronic/* (2 ed.). International Electrotechnical Commission.

ISACA. (2018). *COBIT2019.* Schaumburg: ISACA.

ISO/TS-15066. (2016). *Robots and robotic devices — Collaborative robots* (1 ed.). Switzerland: International Organization for Standardization.

ISO-10218-1. (2011). *Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots* (2 ed.). Switzerland: International Organization for Standardization.

ISO-10218-2. (2011). *Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration.* Switzerland: International Organization for Standardization.

ISO-12100. (2010). *Safety of machinery — General principles for design — Risk assessment and risk reduction* (1 ed.). Switzerland: International Organization for Standardization.

ISO-13849-1. (2015). *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design* (3 ed.). Switzerland: International Organization for Standardization.

Kovacs, E. (03 de 05 de 2017). *Securityweek*. Obtenido de Securityweek: https://www.securityweek.com/industrial-robots-vulnerable-remote-hacker-attacks

Kuka. (23 de 02 de 2018). *Kuka*. Obtenido de Kuka: https://www.fircroft.com/blogs/cobots-will-play-an-important-role-in-helping-to-fill-the-uks-85423123655

Patil, P. (2016). Artificial intelligence incyber security. *International journal of research in computer applications and robotics*, 1-5.

Tanenbaum, A. (2012). *Redes de computadoras* (Quinta ed.). México: Pearson educación.

Univelsal-Robots. (11 de 07 de 2018). *Univelsal robots*. Obtenido de Univelsal robots: https://www.universal-robots.com/about-universal-robots/news-centre/the-history-behind-collaborative-robots-cobots/

Vicentini, F., Ruggeri, M., Dariz, L., Pecora, A., Maiolo, L., Polese, D., . . . Molinari, L. (2014). Wireless sensor networks and safe protocols for user tracking in human-Robot cooperative workspaces. *IEEE*, 1274-1279.