ESPECIALIZACIÓN EN CIBERSEGURIDAD

Estudio para la implementación de las políticas empresariales de ciberseguridad para la conexión a la red de automatización para las plantas industriales de producción de café.

SANTIAGO ALFONSO LÓPEZ LÓPEZ – JULIÁN VÉLEZ ZULUAGA

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

ESTUDIO PARA LA IMPLEMENTACIÓN DE LAS POLÍTICAS EMPRESARIALES DE CIBERSEGURIDAD PARA LA CONEXIÓN A LA RED DE AUTOMATIZACIÓN PARA LAS PLANTAS INDUSTRIALES DE PRODUCCIÓN DE CAFÉ.

Trabajo de grado presentado como requisito para optar al título de *Especialista en Ciberseguridad*

Modalidad de grado: Monografía

Ing. Abg. Héctor Roberto Gordon Quinche

Santiago Alfonso López López – Julián Vélez Zuluaga

UNIVERSIDAD CATÓLICA DE MANIZALES

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESPECIALIZACIÓN EN CIBERSEGURIDAD

MANIZALES, CALDAS

2023

Nota de aceptación 4.7

Agradecimientos

Expresamos nuestro agradecimiento al director de la Especialización Jhon Cesar Arango, por su guía y apoyo constante durante todo el proceso de elaboración de este. Su experiencia y dedicación fueron fundamentales para la realización de este trabajo y su ayuda nos permitió superar los obstáculos y dificultades que se presentaron en el camino.

Esperamos que este trabajo ayude a desarrollar una cultura de seguridad en procesos industriales, para que no tengan repercusiones en su producción.

Finalmente, queremos agradecer a cada uno de los lectores que han dedicado su tiempo para leer nuestra monografía. Espero que el contenido haya sido de su agrado y les haya resultado interesante y útil.

Tabla de Contenido

Listado de Figuras

Listado de Tablas

Resumen

Este trabajo analiza conceptos como ciberseguridad, seguridad de la información y la gestión de riesgos relacionándolos con la conexión de redes de automatización industrial, para poder implementar políticas de conexión a dichas redes tomando como base las empresas Buencafé Liofilizado y DESCAFECOL, ambas con plantas industriales de producción de café en el departamento de Caldas en Colombia. Cada uno de estos conceptos, aplicados a las redes industriales y explica su importancia para garantizar la confidencialidad, integridad y disponibilidad de la información CID en las redes de automatización.

Las redes de automatización (OT Tecnología Operativa) se refieren al uso de hardware y software para monitorear y controlar procesos industriales, dispositivos e infraestructura. La conexión a estas no cuenta con una política que siga una metodología que se centre en los aspectos de la seguridad de la información, incluidos los controles físicos, ambientales, administrativos y de gestión, así como los controles técnicos.

Los riesgos en ciberseguridad cambian a gran velocidad generando la creación de políticas que se adapten a esos cambios y no ser políticas estáticas. Adicional se debe integrar con los sistemas de gestión presentes dentro de la organización para que haga parte del desarrollo diario de la organización y no sea un proceso aislado. El uso del ciclo PHVA (Planear, Hacer, Verificar y Actuar) de la ISO 27001 y el enfoque a riesgos ayudan a la integración, lo que permite la implementación de las políticas de ciberseguridad y lo convierte en un proceso dinámico, sistemático y repetitivo que identifica, califica y evalúa las amenazas a las que está expuesta una organización para tomar las acciones necesarias para eliminar, mitigar, compartir o tratar los riesgos.

Abstract

This study analyses concepts like cybersecurity, information security and risk management relating them to the connection of industrial automation networks, in order to implement connection policies to those kinds of networks, based on BUENCAFE Liofilizado and DESCAFECOL coffee production plants, both located in Caldas, Colombia. It defines each of these concepts as applied to industrial networks and explains their importance in ensuring the confidentiality, integrity and availability of information in automation networks.

The OT (Operational Technology) network refers to the use of hardware and software to monitor and control industrial processes, the connection to those networks does not have a policy that follows a methodology focused on aspects of information security, including physical and environmental, administrative and management controls, as well as technical controls.

Cybersecurity risks change rapidly, so a policy must adapt to these changes and cannot be a static policy. Additionally, it must be integrated with the management systems present within the organization so that it becomes part of the daily development of the organization and is not an isolated process. The use of the PDCA (Plan, Do, Check, Act) cycle o the ISO 27001 and the risk approach, makes easier the integration, which allows the implementation of cybersecurity policies and makes it a dynamic, systematic and repetitive process that identifies, qualifies and evaluates the threats to which an organization is exposed in order to take the necessary actions to eliminate, mitigate, share or manage the risks.

1. Introducción

El café es en la actualidad la segunda bebida más consumida en el mundo después del agua. Su historia se remonta a Etiopía, pero su expansión empezó con los árabes quienes lo extendieron por el denominado “mundo árabe” y luego por Europa en el siglo XVII.

En el siglo XVIII los holandeses y franceses lo trajeron a América llegando a ser un cultivo muy importante para el siglo XIX.

En Colombia el cultivo de este producto inició en la zona de los Santanderes y para 1850 ya se cultivaba en los departamentos de Antioquia, Cundinamarca y Caldas. Para finales del siglo XIX el café se había convertido en el principal producto de exportación del país.

En 1901 Satori Kato, químico de origen américo-japonés, inventó el primer café soluble, presentándolo en la Panamerican Exposition en Nueva York y ya en 1914, durante la primera guerra mundial, los soldados estadounidenses consumían café instantáneo empacado en sobres, pero fue solo hasta la década de los 30 que se desarrolló la producción de este producto a gran escala. (Federación Nacional de Cafeteros de Colombia, s.f.)

En las décadas de los 70 y 80 se construyen en el departamento de Caldas la Fábrica de Café Liofilizado (hoy Buencafé) y Descafecol, con el objetivo de producir café soluble y así generar productos de valor agregado a partir del café colombiano.

La necesidad de incrementar sus capacidades de producción y estandarizar sus procesos, llevó a ambas compañías a implementar la automatización dentro de sus procesos de producción haciendo uso equipos PLC (Control Lógico Programable) que les permiten controlar las máquinas de producción y su procesamiento del producto en las diferentes etapas del mismo.

Con el paso del tiempo, se hizo necesario recopilar datos de estos procesos automatizados y se instalaron sistemas de supervisión, Control y Adquisición de Datos, mejor conocidos como “SCADA” (del inglés, “Supervisory Control and Data Acquisition”).

Los sistemas SCADA permiten tener información centralizada, realizar procedimientos de control a distancia, implementar alarmas, registrar datos para obtener históricos, determinar tendencias, entre otros. (Revista electroindustria, 2016)

Esta tecnología fue inicialmente pensada para estar aislada y utilizaba protocolos de conexión como RS232, Modbus, 485 o DH+, pero a medida que vivimos en un mundo interconectado, se ha hecho necesario acceder a los mismos desde las redes LAN (del inglés Local Area Network) de las compañías y en algunos casos desde dispositivos conectados a internet involucrando otras aspectos como HTTPS, FTP, Ethernet, TCP/IP, etc.

El desarrollo de los dispositivos de automatización y los sistemas SCADA, es más lento en comparación con el de las tecnologías sobre las cuales trabajan las redes LAN e internet; es por ello que cuando se conectan ambas redes, es de suma importancia tener en cuenta la protección de las redes de automatización frente a los ataques de diversos tipos que puedan producirse desde la LAN o internet.

Por eso, desarrollar políticas de ciberseguridad para los sistemas de control industrial es de vital importancia, para estandarizar, evaluar y tomar medidas sobre vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.

Dichas políticas se articulan con los diferentes sistemas de gestión de las compañías desde la gestión de riesgos.

Al ser productoras de alimentos y además exportadoras de los mismos, las empresas productoras de café utilizan sistemas de gestión de riesgos con enfoque a la inocuidad como IFS Food (International Featured Standards en su versión Food) y a la seguridad como BASC

(Business Alliance for Secure Commerce). Las políticas empresariales de ciberseguridad son un complemento y se integran a dichos sistemas tomando la identificación de los peligros y la evaluación de riesgos desde un punto de vista técnicamente más específico y enfocado a la ciberseguridad en la conexión de las redes de automatización industrial.

2. Localizacion

Este trabajo se desarrolla teniendo en cuenta las redes industriales ubicadas en las plantas de producción de café Buencafé Liofilizado y DESCAFECOL, ambas localizadas en el departamento de Caldas en Colombia.

Buencafé Liofilizado posee una planta de producción de liofilización en Chinchiná y DESCAFECOL posee dos plantas de producción una de café soluble y la otra de descafeinación, ambas ubicadas en la zona industrial de Manizales.

3. Objetivo General

Efectuar un estudio para la implementación de las políticas empresariales de ciberseguridad en conexión a la red de automatización para las plantas industriales de producción de café.

3.1 Objetivos Específicos

- Definir una guía para realizar un análisis de riesgos para determinar las vulnerabilidades de las redes de automatización
- Establecer estrategias para definir los controles a implementar para disminuir las vulnerabilidades detectadas entendiendo dichas redes como infraestructura crítica.
- Presentar estrategias de verificación de los controles definidos.
- Considerar los planes de respuesta a incidentes ante la materialización e impacto de los riesgos tecnológicos

4. Antecedentes

La digitalización ha avanzado a niveles sin precedentes en las últimas décadas a nivel corporativo y personal. Las empresas querían utilizar la última tecnología para simplificar y aumentar la producción, pero esto afectó el nivel de seguridad a medida que se exponían más sistemas e información.

La ciberseguridad es fundamental para cualquier negocio que quiera pertenecer a un mundo totalmente interconectado. A pesar de su importancia, pocas organizaciones reconocen las amenazas a sus operaciones en un mundo interconectado y tienen políticas y estrategias claramente definidas para abordarlas.

La ciberseguridad pretende que las empresas protejan sus sistemas informáticos de ataques que pudieran comprometer el buen funcionamiento y mal uso de la información obtenida para obtener ganancias económicas o dañar la reputación. La ciberseguridad no protege solo los equipos informáticos, sino que se abarca cualquier dispositivo o sistema conectado a Internet. El objetivo es enseñar a los usuarios cómo prevenir la pérdida de datos y acciones similares, así como utilizar diferentes métodos de seguridad para prevenir y/o contrarrestar estos ataques. Esta es la razón por la cual las políticas de seguridad cibernética en el gobierno y la industria son tan importantes.

A nivel internacional se reseñan los siguientes antecedentes:

(Alcaraz, Fernández, Román, Balástegui, & López, 2008) en su publicación “Gestión Segura de Redes SCADA” muestran cómo la llegada de nuevas tecnologías a los sistemas SCADA hacen necesario realizar análisis frecuentes de vulnerabilidad para mitigar o evitar ocurrencias y así garantizar la fiabilidad de dichas redes que controlan otras infraestructuras complejas.

En la misma se concluye que para proteger los sistemas SCADA hay que identificar nuevas e importantes necesidades como son: la definición de estándares y políticas de seguridad, especificación de roles y responsabilidades, y diseño e implementación arquitecturas de red segura sin dejar de lado otros factores necesarios como la gestión de riesgos, incidencias y documentos, la definición de métricas y metodologías de evaluación, la proliferación periódica de programas educativos, el mantenimiento y la auditoría.

La publicación citada anteriormente, se relaciona con los objetivos del presente trabajo pues cita la necesidad de tener una política de seguridad formulada para la protección de estos sistemas y determinar los riesgos para implantar recomendaciones que disminuyan la vulnerabilidad de los mismos.

Adicionalmente (Geeta & Kolin, 2021) en su publicación “Architecture and security of SCADA systems: A review” reafirman que muchas infraestructuras críticas son supervisadas por los sistemas SCADA y enumeran algunos de los riesgos a los que se enfrentan.

Concluyen los autores que los sistemas SCADA pasaron de ser sistemas aislados a estar interconectados y a hablar en la actualidad de SCADA en la nube y resaltan que hay problemas de investigación que deben ser resueltos para solucionar los retos de seguridad de este tipo de sistemas.

Esto se relaciona con el proyecto ya que la publicación reafirma la vulnerabilidad de los sistemas SCADA y la necesidad de protegerlos.

5. Marcos de la Investigación

Justificación

El presente trabajo se justifica por la necesidad de implementar una guía de políticas de seguridad en la conexión de redes de control industriales para protegerlas frente a diversos ciberataques. Con el desarrollo del mismo se generarían políticas que permitan a una planta industrial seguir utilizando, modificando y actualizando sus redes de automatización, teniendo un alto nivel de confiabilidad y protegiéndolas de situaciones que pongan en riesgo la continuidad del negocio, calidad del producto, inocuidad de la planta, afectaciones al medio ambiente y la seguridad industrial de los empleados y la comunidad que habitan a sus alrededores.

De la misma manera tener un sistema de automatización confiable, permite a las compañías seguir procesando productos de alta calidad que son insignia de la región, como lo es el café. Esos productos aportan directamente al crecimiento económico e industrial del departamento y de las personas que laboran en ellas, e indirectamente generan una dinámica comercial positiva que impacta a sus proveedores.

Descripción del Problema

La revisión preliminar evidencia que no hay una política de ciberseguridad para la planta de producción en los sistemas de control industrial. Adicionalmente que la red corporativa está interconectada a la red de automatización, exponiéndola a los diferentes tipos de ataques desde la misma corporativa. La red OT es administrada por el área de automatización y la red IT por el área de sistemas. Esta última área no cuenta con una política que siga una metodología de gestión que permita identificar, evaluar y mitigar los riesgos de ciberseguridad generados por la conexión de ambas redes en su estado actual y frente a nuevas implementaciones en la red de

automatización o nuevas amenazas que se presenten desde la red IT enfocadas a atacar la red OT.

Planteamiento del Problema

¿Qué procedimiento se puede seguir para la definición de políticas de ciberseguridad en conexión para la red de automatización de las plantas industriales de producción café, en la vulnerabilidad de las mismas frente a diferentes ataques?

Marco Normativo.

En el contexto geográfico en el que se desarrolla este proyecto, no hay normas legales que sean aplicables en Colombia, sin embargo, durante el desarrollo del mismo se hace uso de diferentes conceptos y procesos contenidos en normas internacionales enfocadas en la seguridad de la información y la gestión de riesgos.

La ISO 27032 provee una guía macro de la ciberseguridad teniendo en cuenta puntos clave como las políticas, controles, las vulnerabilidades, los ataques, sus agentes y los activos con un enfoque en el ciberespacio (redes privadas e internet).

El Marco de Referencia de la ISO 31000 con su administración de riesgos con uso del ciclo PHVA, sirve como apoyo para la gestión de riesgos que presenta el proyecto en su enfoque al aseguramiento de las conexiones entre las redes de automatización y las administrativas.

Las normas BASC e IFS Food también son referenciadas puesto que las plantas de producción donde se enfoca el proyecto son procesadoras de alimentos certificadas en ambas y es importante tener en cuenta los parámetros de las mismas.

De igual manera se tienen en cuenta aspectos de continuidad de negocio como la capacidad de seguir trabajando luego de un incidente, tema que es abordado por la norma ISO

22301 proporcionando un marco para seguir funcionando durante situaciones no esperadas como es el caso de los incidentes de ciberseguridad.

Marco Teórico-Conceptual

Tecnología Operacional (Operational Technology OT)

De acuerdo a FORTINET (FORTINET, s.f.) la definición de Tecnología Operacional (OT) es “el uso de hardware y software para monitorear y controlar procesos físicos, dispositivos e infraestructura”.

La tecnología OT se dedica a detectar cambios en los procesos físicos a través de la monitorización y control de dispositivos.

Definición de Ciberseguridad

De acuerdo con la Norma ISO 27032:2012 se define la ciberseguridad como “Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio”.

Se define el ciberespacio como un entorno complejo que resulta de la interacción de las personas, el software y servicios a través de internet, por medio de dispositivos tecnológicos y redes interconectadas, que no existe en forma física.

Seguridad de la Información

Para establecer la diferencia con la seguridad de la información, se deben revisar algunos conceptos que nos permiten tener el contexto general. Según la Real Academia Española (RAE), la seguridad se puede definir como: “Libre o exento de todo peligro, daño o riesgos”. Sin embargo, es una condición ideal, ya que en la realidad no es posible tener la certeza de que se puedan evitar todos los peligros.

El principal propósito de la seguridad en todos los ámbitos de aplicación es el de reducir riesgos hasta un nivel que se pueda aceptar y mitigar las amenazas latentes.

En un Sistema de Gestión de Seguridad de la Información ISO 27001 (ISO, 2013) la información se puede almacenar, procesar o transmitir de diferentes maneras:

- De forma digital
- De forma verbal
- Mensajes escritos
- Mensajes Impresos

En seguridad de la información es de vital importancia catalogar los datos de acuerdo con su criticidad e importancia, con el fin de que las protecciones se definan de forma adecuada sin importar el formato en que se encuentren.

Riesgos en los SCADA

GUÍA DE SEGURIDAD DE LAS TIC, (CCN-STIC-480), SEGURIDAD EN SISTEMAS SCADA. Centro Criptológico Nacional, España, 2010. Presenta un procedimiento para analizar riesgos de los sistemas SCADA, sus vulnerabilidades, impacto y necesidades en las entidades estatales españolas.

Gestión de Riesgos

La norma ISO 31000 es una norma publicada por la International Standard Organization (ISO) y se encuentra en su segunda versión publicada en 2009. Esta norma presenta los principios y directrices para realizar la gestión de los riesgos dentro de las organizaciones. Fue adoptada en Colombia a través del ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación) como la NTC-ISO 31000 en el 2018. (ICONTEC, 2018)

La evaluación de riesgos según ISO 31000:2018 es un proceso dinámico, sistemático y repetitivo que pretende identificar, calificar y evaluar las amenazas a las que está expuesta una organización, con el fin de tomar las acciones necesarias para eliminar, mitigar, compartir o tratar los riesgos.

En el caso de la ciberseguridad, las evaluaciones de riesgos se centran en todos los aspectos de la seguridad de la información, incluidos los controles físicos y ambientales, administrativos y de gestión, así como los controles técnicos (ISO, 2013).

Continuidad del negocio

La norma ISO 22301 presenta los principios y directrices para la continuidad del negocio y se enfoca en la capacidad de las compañías para seguir produciendo o brindando servicios a unos niveles aceptables luego de una situación perjudicial o catastrófica. Se encuentra en su segunda edición, publicada en el año 2019 por la International Standard Organization (ISO) (International Standard Organization, 2019)

BASC

La certificación BASC es emitida por la World Basc Organization y a través de sus diferentes capítulos en el mundo. La versión actual es la 5 y está enfocada a la evaluación de riesgos desde la perspectiva del comercio y la seguridad de la carga, sin dejar de lado la evaluación de los demás riesgos a los que la empresa se ve expuesta y para la versión que está en proceso de publicación se incluyó el concepto de ciber amenaza. (World Basc Organization)

IFS Food

Es una norma de seguridad alimentaria implementada por el International Featured Standards. Actualmente se encuentra en su versión 7 y dentro de sus principales características se encuentran que tiene un enfoque basado en el riesgo identificando los peligros y riesgos

específicos de la empresa. Su enfoque es en alimentos y las empresas que los producen y está disponible en 5 idiomas (International Featured Standards, s.f.)

Ciclo de Deming o PHVA

Es una metodología implementada por Edward Deming para implementar soluciones con base en la mejora continua. Tiene 4 fases cíclicas que se van ejecutando reiteradamente y son planear, hacer, verificar y actuar, de ahí que se le conozca también como ciclo PHVA. (sydle.com, 2021)

6. Metodología

La metodología sobre la que se desarrolla este proyecto es la PHVA o Ciclo de Deming. Esta metodología cualitativa plantea 4 fases a desarrollar denominadas Planear, Hacer, Verificar y Actuar que son desarrolladas de manera progresiva pero que al llegar al terminar su última fase (Actuar) se reinicia. Lo anterior para generar lo que se denomina mejora continua.

El desarrollo del proyecto se da pasando por cada una de las fases y generando actividades enfocadas a la creación de una política de ciberseguridad en la interconexión de redes de automatización a redes administrativas en plantas de procesamiento de café, que permita que el resultado de cada una de las fases sirva como insumo para el desarrollo de la siguiente y teniendo el análisis y gestión de los riesgos como el punto central del desarrollo del ciclo.

7. Cuerpo del trabajo

Políticas Empresariales de Ciberseguridad para la Conexión a la Red de Automatización para las Plantas de Producción de Café

La implementación de políticas empresariales de ciberseguridad para la conexión a la red de automatización para las plantas de producción de café, debe partir de la identificación del contexto de trabajo de dichas empresas, las políticas deben responder a las necesidades específicas y las realidades de la empresa. En el caso de Buencafé Liofilizado y Descafecol son productoras de alimentos y una gran parte de su producción es dedicada a la exportación, por lo que poseen implementados sistemas de gestión como IFS y BASC que utilizan el ciclo de mejora PHVA (Planificar - Hacer - Verificar - Actuar) en que los procesos iteran regularmente las 4 fases con el objetivo de revisar lo hecho en la iteración anterior y generar una mejora continua.

El uso del ciclo PHVA de mejora continua además permite que las políticas se revisen y ajusten constantemente y no se conviertan en un documento estático que se desarrolló para responder a las necesidades de un momento específico, pero que no corresponde con la realidad actual.

Los riesgos en ciberseguridad cambian a gran velocidad por lo que una política estática no es funcional, es necesario además que la política de ciberseguridad se integre y armonice con los sistemas de gestión presentes dentro de la organización para que haga parte del desarrollo diario de la organización y no sea un proceso aislado adicional. El uso del ciclo PHVA y el enfoque a riesgos ayudan a la integración. Es de notar que además normas como BASC en su versión 6 - 2022 ya tiene dentro de sus estándares requisitos específicos para ciberseguridad y requiere integrar el componente de ciberseguridad explícitamente dentro de la política de seguridad, lo que muestra la necesidad de tomar en cuenta dichas normas para no realizar definiciones dobles o hasta en el peor de los casos discordantes.

Etapa de Planear.

Dentro de la etapa de planificación, es necesario tener en cuenta el contexto de la organización. El contexto nos muestra un panorama general con información acerca de la organización y según la norma ISO 31000 se deben tener en cuenta aspectos externos que aplican a todas o casi todas las compañías del mismo sector como:

- Las leyes que la rigen
- Las tendencias de la tecnología
- Las normativas de instituciones públicas o privadas que la afecten.

Es necesario además definir un contexto interno que es específico para la compañía, algunos ejemplos son:

- Normas que tiene adoptadas la compañía (pueden ser de calidad, seguridad, inocuidad, gestión ambiental, etc).
- La estructura organizacional.
- Los recursos físicos, humanos y tecnológicos.

El propósito de la definición del contexto es que la política sea ajustada a la realidad y especificidad de la empresa y no se trate de implementar alguna genérica que no corresponda al marco de trabajo de la compañía.

El punto de recursos es muy importante; se debe conocer el sistema de automatización que se tiene implementado y los flujos de información desde y hacia otras redes.

Es por ello que es necesario realizar un inventario de los equipos con los que cuenta el sistema de automatización. Este inventario debe contar con el listado de los PLCs, conmutadores y demás equipos incluyendo su marca y los equipos con los que tiene interacción. Debe también enumerar cuales son los puntos de interconexión física con otras redes y cómo es su interacción lógica. La ejecución del inventario y clasificación de los activos de información, la realiza un

grupo interdisciplinario que debe contar con participantes del área donde se encuentra el activo, y personal de procesos estratégicos, operativos y de soporte.

La Tabla 1 presenta un ejemplo de formato para la realización del inventario. De igual manera se debe realizar el inventario de los SCADA con su marca, protocolos y a que equipos supervisa. La Tabla 2 muestra una propuesta para este inventario.

Tabla 1

Formato inventario equipos sistema de automatización.

INVENTARIO DE EQUIPOS RED DE AUTOMATIZACIÓN											
# Item	Código Equipo	Nombre equipo	Proceso en el que se encuentra	Proceso Anterior	Proceso Posterior	Conectado a	¿Es punto de Interconexión con red administrativa?	Disponibilidad (importancia que tiene la ausencia del activo)	Integridad (qué repercusiones tendría la modificación de este activo sin la autorización pertinente)	Confidencialidad (cual sería la importancia del acceso del activo sin autorización)	Acceso (defina quien debe tener acceso de lectura (L) o modificación (M))
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											

Tabla 2

Formato de inventario programas SCADA

INVENTARIO PROGRAMAS SCADA RED DE AUTOMATIZACIÓN										
# Item	Código Programa	Nombre Programa	Proceso en el que se encuentra	Marca	Protocolo de comunicación	Equipos que supervisa	Disponibilidad (importancia que tiene la ausencia del activo)	Integridad (qué repercusiones tendría la modificación de este activo sin la autorización pertinente)	Confidencialidad (cual sería la importancia del exceso del activo sin autorización)	Acceso (defina quien debe tener acceso de lectura (L) o modificación (M)) (cual sería la importancia del exceso del activo sin autorización)2
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										

Los criterios de disponibilidad, integridad y confidencialidad al igual que los niveles de clasificación pueden ser definidos por la organización con base en sus necesidades, sin embargo, el Ministerio de las Tecnologías de la Información y las Telecomunicaciones de Colombia (MINTIC) en su Guía para la Gestión y Clasificación de Activos de la Información (Ministerio de las Tecnologías de la Información y las Telecomunicaciones de Colombia, 2016), presenta un criterio de 4 niveles para cada propiedad como lo muestra la Tabla 3 y una clasificación de 3 niveles como se puede ver en la Tabla 4:

Tabla 3

Criterios de clasificación.

CRITERIOS DE CLASIFICACIÓN		
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
Confidencial	Alta	Alta
Privado	Media	Media
Público	Baja	Baja
No clasificado	No clasificado	No clasificado

Nota. Adaptado de la Guía para la Gestión y Clasificación de Activos de la Información MINTIC https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Tabla 4

Niveles de clasificación.

NIVELES DE CLASIFICACIÓN	
ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Nota. Tomado de la Guía para la Gestión y Clasificación de Activos de la Información MINTIC https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

De igual manera se hace necesario definir en el formato quienes tendrán acceso a los activos de información y su tipo de acceso (de lectura o modificación). Quien no se encuentre listado dentro de los accesos no debe accederlos.

Los formatos de inventarios de equipos de automatización y programas SCADA pueden ser estructurados y diligenciados en una hoja de cálculo, esto tiene ventajas desde el punto de vista del acceso y la comunicación pues se puede permitir el acceso y consulta de los mismos para las personas involucradas, se facilita además el manejo documental y desde el punto de vista ambiental se disminuye la huella de carbono asociada a la impresión de estos.

Tener estos inventarios nos permite conocer los flujos de información entre la red de automatización y las otras redes para determinar un inventario de riesgos a los que están expuestas para después evaluar el riesgo de los mismos.

Estos riesgos en nuestro caso deben estar relacionados con la ciberseguridad pues el estudio y evaluación de otro tipo de riesgos no es parte del alcance de este documento.

Las columnas de disponibilidad, integridad y confidencialidad son un insumo importante para la realización del inventario de peligros y su posterior evaluación de riesgos.

Se deben tener en cuenta la mayor cantidad de peligros posibles tratando de abarcar todos los posibles sin importar que se tomen como despreciables. Ya en fases posteriores se determinará su nivel de riesgo y si se deben generar controles o se asumen.

También en esta etapa de planeación se recopila información acerca del recurso humano que opera el sistema de automatización documentos firmados relacionados con aspectos legales como acuerdos de confidencialidad u otros que tendrán relevancia frente a los planes de respuesta a incidentes.

Etapa Hacer

El paso “Hacer” es el momento para evaluar los riesgos identificados inicialmente y definir sus controles. Esta etapa debe realizarse a pequeña escala, en un entorno controlado. No debe verse afectada por factores externos ni interrumpir otros procesos u operaciones del proceso productivo. Naturalmente, el objetivo de esta etapa es recopilar datos e información sobre el impacto de la prueba, ya que esto indicará los controles a implementar.

Identificación.

Teniendo en cuenta el inventario de equipos del sistema de automatización que se realizó en la tabla 1 y el inventario de programas SCADA de la tabla 2, se debe realizar el proceso de

identificación de las vulnerabilidades presentes en los mismos de acuerdo con las que se presentaron anteriormente. Este proceso se denomina identificación y su objetivo es determinar todas las posibles fallas que se puedan presentar (desde el punto de vista de la ciberseguridad) para luego pasar a analizarlas y valorarlas. Se deben incluir todas las posibles vulnerabilidades sin llegar a demeritar ninguna porque el no considerarla puede llevar a que se materialice algún riesgo. En las etapas de análisis y valoración se determinará el nivel de importancia de esa vulnerabilidad y que tanto la debemos controlarla.

Es importante tener en cuenta que, si bien algunas vulnerabilidades pueden mitigarse, otras no y, como resultado, deben aceptarse y gestionarse mediante el uso de un tipo alternativo de contramedida.

La publicación del NIST 800-82 Revisión 2 agrupa las vulnerabilidades en: Vulnerabilidad de plataforma, Vulnerabilidades de red y Vulnerabilidades a nivel de políticas y procedimientos.

Es importante tener en cuenta que, si bien algunas vulnerabilidades pueden reducirse, otras no pueden y, como resultado, deben aceptarse y gestionarse mediante el uso de un tipo alternativo de contramedida.

Dado que tienen un impacto en el hardware, el software o las comunicaciones de los dispositivos, las dos primeras entran en la categoría de vulnerabilidades técnicas o tecnológicas. La tercera categoría tiene un impacto en la organización en su conjunto, el marco de gestión de la seguridad y las reglas y directrices establecidas para tratar con los sistemas de automatización y control, específicamente para garantizar su seguridad y protección.

Algunos de los riesgos y vulnerabilidades potenciales identificados por este grupo incluyen:

1.- Vulnerabilidades y riesgos de políticas y procedimientos.

- Medidas de seguridad insuficientes.

- Falta de iniciativas de sensibilización y formación.

- La falta de guías adecuadas para la implementación de sistemas de control industrial.

- Falta de controles administrativos para imponer normas de seguridad.

- Revisiones insuficientes de las medidas de seguridad.

- Planes de contingencia generalizados.

- Protocolos y planes deficientes de respuesta a incidentes.

2.- Riesgos y Vulnerabilidades en los Sistemas de Control.

2.1. - Arquitectura y diseño vulnerables.

- Inadecuada integración del concepto de seguridad en las etapas de diseño y arquitectura operativa de los sistemas industriales que son impulsados por intereses comerciales (productividad) sin tener en cuenta consideraciones de seguridad.

- Un perímetro de red poco claro.

- Tráfico de red de ICS y otros dispositivos que utilizan la misma infraestructura de red.

- Servicios no regulados. Por ejemplo, DNS, DHCP, NTP, etc.

- Manipulación y almacenamiento inadecuado de logs.

2.2. - Vulnerabilidades en Configuración y Mantenimiento.

- La gestión de configuración excluye hardware, software y firmware.

- Software o sistemas operativos que ya no son compatibles con el fabricante o para los que no se han creado nuevos parches para vulnerabilidades conocidas.

- Pruebas insuficientes sobre cambios relacionados con la seguridad.

- Falta de precauciones de seguridad o controles de acceso remoto insuficientes.

- Configuraciones de equipos críticos sin copias de seguridad.

- La creación de contraseñas no se rige por políticas y procedimientos.

- Implementación inadecuada de control de acceso a dispositivos.

- Replicación de datos entre sistemas innecesarios o sin el uso de controles de seguridad.

- Sin software antivirus o desactualizado.

- La implementación de software antivirus sin realizar las pruebas adecuadas, lo que podría afectar el rendimiento o la funcionalidad.

- El uso de software propenso a ataques de denegación de servicio.

- No instalar sistemas IDS/IPS.

2.3. Riesgos y Vulnerabilidades Físicas.

- Acceso físico a los dispositivos por parte de personas no autorizadas.

- La presencia de señales electromagnéticas, picos de tensión y cargas que puedan interferir en el funcionamiento o dañar el equipo.

- La pérdida de suministro eléctrico de respaldo.

- Pérdida de control sobre factores ambientales como la humedad, la temperatura y el polvo en suspensión.

– Puertos físicos desatendidos.

2.4. - Riesgos y Vulnerabilidades en el Desarrollo de Software.

- Validación de datos insuficiente.

- No existen medidas de seguridad o están apagadas.

- Utilización inapropiada o incorrecta de técnicas de autenticación, control de acceso y privilegios.

2.5. - Riesgos y Vulnerabilidades en las Comunicaciones y Red.

- La aprobación innecesaria de comunicaciones entre sistemas de control.

- Cortafuegos mal configurados o inexistentes.

- La ausencia de registros de enrutador o firewall que puedan contener detalles sobre las causas de un incidente.

- Haciendo uso de la red servicios que envían datos en texto plano.

- El uso de protocolos débiles sin autenticación de punto final, cifrado de comunicaciones o control de integridad de mensajes.

- Débiles métodos de autenticación y cifrado de información entre dispositivos y puntos de acceso en redes inalámbricas.

Análisis.

Al tener ya el listado de las vulnerabilidades, pasamos de realizar el análisis. En éste se determina la consecuencia de que la vulnerabilidad sea utilizada, es decir, se materialice el riesgo y determinamos qué variable se ve afectada desde la seguridad.

Las 3 variables a tener en cuenta son:

- Confidencialidad: la información es accesible de forma única a las personas que se encuentran autorizadas.

- Integridad: la información se mantiene inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización
- Disponibilidad: el sistema se mantiene trabajando sin sufrir ninguna degradación en cuanto a accesos.

En la materialización de un riesgo se pueden afectar una o varias de las variables.

Luego de realizar el análisis de riesgos, es necesario iniciar la implementación de medidas de mitigación de las vulnerabilidades.

Valoración.

Las fases anteriores permiten tener el panorama de los elementos que componen el sistema de automatización y los riesgos a los que están expuestos. Lo que se debe hacer luego es valorar ese riesgo para lo cual se deben tener en cuenta 3 aspectos:

- Frecuencia: que tantas veces se realiza la actividad vs el número de días de trabajo para determinar el nivel de exposición a la amenaza. Se debe entonces realizar el siguiente cálculo: $Días\ en\ que\ se\ ejecuta\ la\ actividad\ /\ número\ de\ días\ trabajados$ y el resultado se se compara contra el criterio descrito en la siguiente tabla:

Tabla 5

Criterio de frecuencia

FRECUENCIA		
VALOR	**RANGO**	**CRITERIO**
3	Alta	Mayor a 0.5
2	Media	Mayor a 0.2 y menor a 0.5
1	Baja	Menor o igual a 0.2

- Impacto: que tan grande es la afectación si se materializa el riesgo que estamos evaluando. El criterio se encuentra en la siguiente tabla.

Tabla 6

Criterio de impacto

IMPACTO		
VALOR	**RANGO**	**CRITERIO**
3	Severo	El proceso no puede operar y para su recuperación son necesarios recursos externos
2	Moderado	El proceso no puede operar, pero su recuperación se realiza con recursos disponibles dentro de la compañía
1	Leve	El proceso puede operar

- Alcance: a que parte de la compañía afecta la materialización del riesgo que se está evaluando. El criterio se encuentra en la tabla 7.

Tabla 7

Criterio de alcance

ALCANCE		
VALOR	**RANGO**	**CRITERIO**
3	Global	Supera los límites de la entidad
2	Local	Afecta a más de un proceso
1	Puntual	Afecta solo al proceso

Administración del riesgo.

Luego de valorar los riesgos comienza la etapa de administración de estos. Administrar un riesgo implica inicialmente determinar en qué parte de la zona de riesgo se encuentra el mismo. La zona de riesgo nos indica si un riesgo es alto, medio o bajo y esto se calcula con resultado de la suma de los 3 valores de frecuencia, impacto y alcance dando una ponderación del 20% a la frecuencia, un 50% al impacto y un 30% al alcance, es decir, $(Frecuencia * 0.2) + (Impacto * 0.5) + (Alcance * 0.3)$. El resultado se compara con el criterio presentado en la tabla 8:

Tabla 8

Criterio zona de riesgo

ZONA DE RIESGO		
VALOR	**RANGO**	**CRITERIO**
Alto	Mayor o igual a 2.5	supera los límites de impacto y alcance afectando las actividades. Se deben establecer controles adicionales
Medio	Mayor a 2 y menor a 2.5	se encuentra en los límites permisibles en cuanto a impacto y alcance. Se debe evitar que el riesgo se materialice implementando los controles adecuados
Bajo	Menor a 2	Se encuentra dentro de los rangos establecidos en cuanto alcance e impacto permitiendo asumir el control del riesgo.

Nota. Tomado de MINTIC https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150516:Guia-de-gestion-de-riesgos

La zona de riesgo nos permite valorar entonces ese riesgo para enfocar los recursos en el tratamiento de los que se encuentran con valor medio y alto sin dejar de lado los que están con un valor bajo.

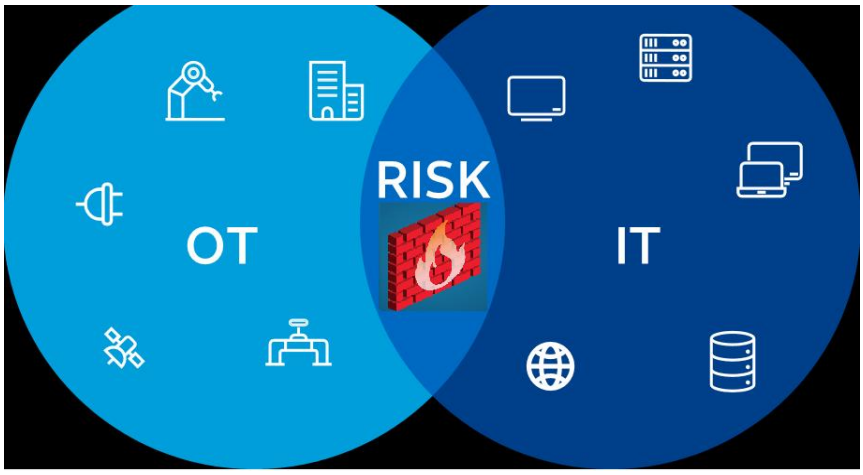
El siguiente paso en la administración de los riesgos es implementar controles que mitiguen los mismos. Estos controles pueden ser técnicos, administrativos o de personal.

Los controles deben estar enfocados a lo definido en el análisis y valoración del riesgo y su objetivo es mitigar los mismos. Un control puede mitigar uno o más riesgos identificados, un ejemplo de ello es la separación y segmentación de redes.

Cuando hablamos de dividir nuestras redes, nos referimos a crear un límite entre la red corporativa, donde ubicamos las redes de TI convencionales como un entorno de "oficina", y nuestra red de automatización o control. Esto lo conseguimos añadiendo un elemento de seguridad perimetral, a modo de Firewall (Corfafuegos), que sólo permite las comunicaciones que son absolutamente necesarias. El hecho de que estos dispositivos sean firewalls de última generación (NGFW, Next Generation Firewall) con funciones IPS/IDS, Antivirus y Application Control y soporte para protocolos de nivel industrial como Profinet, Modbus-TCP, OPC, DNP3, ICCP, devicenet, etc. Es decir, si nuestro objetivo es encontrar amenazas específicas de los sistemas de control, no nos merece la pena realizar únicamente DPI (Deep Packet Inspection) sobre FTP, DNS y HTTP (que también son obligatorios). No debemos pasar por alto el hecho de que estos dispositivos introducen latencias. Como resultado, dependiendo del campo de la automatización, podemos introducir retrasos que no son manejables.

Figura 1

Separación de redes OT de IT



Nota. Adaptado de https://cybersecurity.att.com/blogs/security-essentials/preparing-for-it-ot-convergence-best-practices

La red de control debe tener todos los recursos necesarios (servidores de almacenamiento, DNS, NTP, etc.) al mismo tiempo, pero lamentablemente no siempre es así.

La mejor opción, que se puede usar para separar completamente las redes lógicas y físicas, es usar redes físicas completamente diferentes. Cada comunicación entrante y saliente entre la red corporativa y las redes de "Automatización" está controlada por un punto de seguridad como el NGFW (firewall de próxima generación) descrito anteriormente porque ambos entornos se basan en su propia topología y no comparten componentes de red como conmutadores o enrutadores

La ventaja de esta solución es que cada uno puede realizar su actividad de forma única a nivel de infraestructura. Por tanto, para seguir asegurando la comunicación en caso de cambio o migración de entorno, sólo es necesario modificar el elemento de acoplamiento al Firewall. Esto es particularmente crucial dado que los entornos de OT suelen tener ciclos de vida de los equipos mucho más largos que los entornos de TI.

Las reglas en el NGFW (next-generation firewall) hacen parte de los controles permitiendo filtrar los protocolos anteriormente mencionados (Profinet, Modbus-TCP, OPC, DNP3, ICCP, devicenet, etc), permitir o rechazar conexiones de las redes, equipos autorizados, puertos definidos, y demás aspectos en el tráfico que fluye entre la red OT y la red IT.

El portal Redes Zone indica que la segmentación de la red genera una capa adicional de seguridad, esta se produce en la capa cuatro del modelo OSI, la capa de transporte mejora el rendimiento de la red, y las características de seguridad. “La segmentación funciona mediante el control de tráfico en todas las partes de la red, puede optar por detener todo el tráfico en una parte que quiere alcanzar otra. O bien, puede limitar el flujo que se da en la red por el tipo de tráfico, origen, destino y otras opciones más. La segmentación de red también nos sirve para

agrupar de manera lógica los activos, recursos y aplicaciones por secciones que pueden protegerse bajo protocolos de seguridad específicos" (Zone, s.f.).

Luego de implementar los controles requeridos, es necesario valorar los mismos para realizar la valoración final del riesgo. Los controles se valoran de acuerdo con los criterios presentados en la Tabla 9.

Tabla 9

Criterio de valoración del control

VALORACIÓN DEL CONTROL		
VALOR	**RANGO**	**CRITERIO**
3	Inefectivo	El control no existe, o existe, pero no se aplica, o existe y se aplica, pero el mismo no es efectivo.
2	En Prueba	El Control existe y está en implementación, pero aún no se evidencia su efectividad.
1	Efectivo	El control existe y se aplica de manera efectiva, asegurando la no materialización del riesgo

Nota. Tomado de Guía MINTIC https://cucutanortedesantander.micolombiadigital.gov.co/sites/cucutanortedesantander/content/files/000061/3048_riesgo-gestion-de-tecnologias-de-la-informacion/

En la valoración final del riesgo se determina si ese riesgo es aceptable, moderado o inaceptable. Si un riesgo se valora como inaceptable, se deben implementar más controles que lo lleven a una valoración moderada o aceptable y los que tienen una valoración moderada deben tener un seguimiento permanente.

La valoración se calcula como $Calificación\ del\ riesgo * Valoracion\ del\ control$ y el resultado se toma contra el criterio presentado en la Tabla 10.

Tabla 10

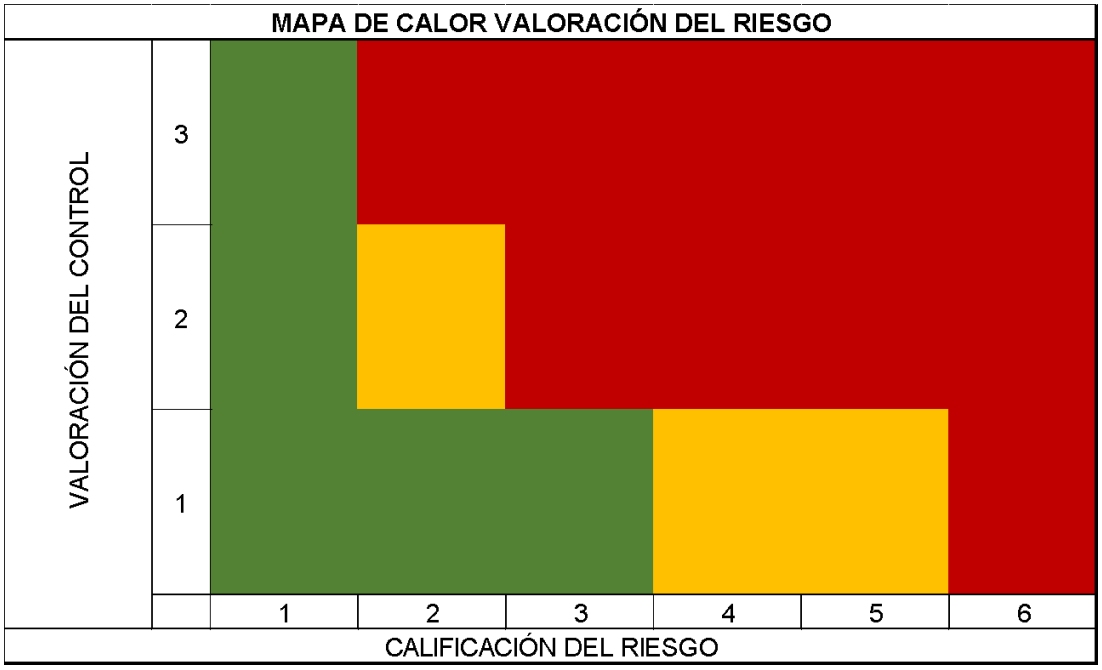
Criterio de valoración del riesgo

VALORACIÓN DEL RIESGO		
VALOR	**RANGO**	**CRITERIO**
Inaceptable	Mayor a 6	No asegura que la materialización del riesgo no se presente, por lo cual se deben ejecutar acciones para incrementar la efectividad del control (reevaluación, adición de nuevos, etc).
Moderado	Mayor a 3 y menor a 6	Debe evaluarse mediante auditorías o seguimiento permanente con el fin de garantizar el resultado satisfactorio del proceso mediante la mitigación del riesgo.
Aceptable	Menor a 3	Ya la entidad evaluó el control y se está asegurando el resultado del proceso, el riesgo no se ha materializado y mediante la aplicación de estos controles se puede asegurar que el riesgo es aceptable y se controlará a través de seguimiento de auditorías de gestión y externas.

Nota. Tomado de MINTIC https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150516:Guia-de-gestion-de-riesgos

Figura 2

Mapa de calor valoración del riesgo



Hay que recordar que todo este proceso es cíclico y dinámico, estas evaluaciones deben realizarse de forma periódica, cuando haya un cambio en los sistemas o cuando se materialice un riesgo para verificar sus cambios al igual que los controles que se tienen identificados. Una revisión puede cambiar el valor en cualquiera de los pasos cambiando un criterio y esto es normal pues la gestión de los riesgos al igual que los sistemas es dinámica.

Para tener una idea unificada y aclarar la identificación, análisis, valoración y administración de los riesgos, presentamos en la Tabla 11 un ejemplo de un formato que unifica todos los conceptos y evalúa 2 riesgos del proceso de Torrefacción (tostión de café). Las últimas 2 columnas del formato se refieren a las acciones que se toman cuando se materializa un riesgo, pero este punto se desarrollará en la etapa del actuar.

Tabla 11

Formato identificación, análisis, valoración y administración de riesgos

FORMATO IDENTIFICACION, ANÁLISIS, VALORACION Y ADMINISTRACIÓN DE RIESGOS																
IDENTIFICACION DEL RIESGO						ANALISIS DE CALIFICACION Y VALORACION				ADMINISTRACION DEL RIESGO						
Área de producción	Equipo/Programa	Actividad	AMENAZA / CAUSA	CONSECUENCIA / RIESGO	VARIABLE AFECTADA	FRECUENCIA	IMPACTO	ALCANCE	CALIFICACION (9+10+11)	ZONA DE RIESGO	CONTROL	VALORACION DEL CONTROL	RIESGO Vs. CONTROL	VALORACION DEL RIESGO	ACCIONES QUE SE DEBEN ADELANTAR EN CASO DE MATERIALIZACION DEL RIESGO	RESPONSABLES
TORREFACCION	PLC controlesadora	Comunicación del PLC con las tostadoras	Pérdida de comunicación del PLC por DoSproveniente de la red administrativa	Pérdida de control de las tostadoras posibilidad alta de incendio	DISPONIBILIDAD	3	3	1	2.4	MEDIO	Firewall de interconexión automatización - administración	1	2.4	ACEPTABLE	Llevar el proceso a control manual y aislar la red de automatización de tonelización de la administrativa para garantizar el funcionamiento de las maquinas y no afectar el proceso productivo. Identificar la fuente de la denegación y bloquearla	Personal área de TI y Personal área de automatización y control
TORREFACCION	PLC control transporte neumático de café	Comunicación del PLC con el sistema de transporte neumático de café	Pérdida de comunicación del PLC por DoSproveniente de la red administrativa	Imposibilidad de transportar el café desde y hacia la sección	DISPONIBILIDAD	3	1	2	1.7	BAJO	Firewall de interconexión automatización - administración	1	1.7	ACEPTABLE	Llevar el proceso a control manual y aislar la red de automatización de tonelización de la administrativa para garantizar el funcionamiento de las maquinas y no afectar el proceso productivo. Identificar la fuente de la denegación y bloquearla	Personal área de TI y Personal área de automatización y control

Etapa Verificar

En la etapa Verificar se tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del sistema. Se evalúa el resultado de la ejecución del plan para saber si este realmente ha sido efectivo o si, por el contrario, no se obtuvieron los resultados esperados.

Después de tener identificadas las vulnerabilidades y realizar el análisis de riesgos, debemos poner a prueba nuestro sistema realizando pruebas a los controles definidos para verificar la eficacia de estos. Una de las pruebas más utilizadas son las de penetración (Pentesting).

Una prueba de penetración o pentesting, es (como su nombre lo indica) una prueba para ingresar a un sistema y detectar vulnerabilidades y saber su alcance y sus posibles consecuencias en dispositivos y aplicaciones. Con ello se puede realizar una evaluación de los controles implementados.

De acuerdo con la información de partida pueden clasificarse en:

Auditorías de caja negra o Black box: no se proporciona ninguna información al auditor, no se especifican los sistemas a auditar. Es un análisis que puede ser altamente invasivo a los sistemas de control.

Auditorías de caja blanca o White box: se proporciona toda la información al auditor, topología de la red, servicios funcionales en los servidores, programas instalados, etc. El objetivo es que la auditoría sea lo más completa posible y detectar el mayor número de vulnerabilidades.

Auditorías de caja gris o Gray box: Es el intermedio entre negra y blanca. Se entrega cierta información al auditor para que se centre en la misma. Puede disminuir los tiempos de los análisis.

Figura 3

Etapas del Pentesting.

Nota. Fuente:

https://www.exevi.com/soluciones/servicio-pentesting-de-webs-apps-y-sistemas/

Existen varias metodologías para la ejecución de la auditoría de pentesting (ISSAF, PCI, PTF, PTES, OWASP, OSSTMM) que se diferencian por el tipo de sistema que se va a auditar o de los requisitos propios que le aplican a la empresa, todas ellas pueden ser realizadas por personal interno de la organización que tengas los conocimientos suficientes de los controles y de la red de automatización y de la red corporativa o con compañías externas especializadas.

Estas son las fases recomendadas para realizar el pentesting enfocado a la verificación de los controles implementados para la interconexión entre la de automatización y la red corporativa.

1.Recopilación de información: reunir la mayor cantidad de información posible sobre el sistema en el que se está probando el control para que la auditoría sea lo más completa y real posible. Recopilar más información permite tratar de vulnerar el control más fácilmente.Para esto podemos utilizar las siguientes herramientas:

WIRESHARK: analizador de protocolo de red ampliamente utilizado en el mundo. Permite ver lo que sucede en su red a un nivel microscópico y es el estándar de facto en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas. (Wireshark, s.f.)

SolarWinds: SolarWinds Network Performance Monitor (NPM) es una sólida aplicación de monitoreo de redes que le permite detectar, diagnosticar y resolver rápidamente cortes y problemas de rendimiento de la red. (SolarWinds, s.f.)

2. Escaneo de vulnerabilidades: luego de la recopilación extensa de información, ésta se utilizará para identificar puntos a atacar y como llegar a ellos al igual que determinar cuáles son sus vulnerabilidades. Para esto podemos utilizar algunas herramientas como:

Nessus: es un programa de escaneo de vulnerabilidades en diversos sistemas operativos, es desarrollada y mantenida por Tenable. (Tenable, s.f.)

Nexpose: es un software de pago, desarrollado por la empresa de ciberseguridad, Rapid7, que sirve para escanear las vulnerabilidades de un sistema o una red. Más allá de dicha función, que también se encuentra en softwares gratuitos, Nexpose sirve para automatizar el monitoreo de un sistema por medio de dichos escaneos. Nexpose clasifica las vulnerabilidades

según su riesgo, sirve para gestionarlas y actualiza los datos del sistema constantemente. (Rapid 7, s.f.)

NMAP: es un software de código abierto que se utiliza para escanear una red y sus puertos con el objetivo de obtener información importante sobre la misma para controlar y gestionar su seguridad. Es una aplicación que se utiliza normalmente para realizar auditorías de seguridad y monitoreo de redes. (Nmap, s.f.)

3.Explotación de vulnerabilidades: cuando se tienen detectadas las vulnerabilidades, se continúa con la explotación de éstas. Para ello, se usan vulnerabilidades identificadas o utiliza credenciales previamente obtenidas para acceder y explotar sistemas. Para esto se puede utilizar una distribución de Linux llamada Kali, para realizar la explotación de estas. Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.

4. Resultado de la revisión de controles: se deben documentar las vulnerabilidades identificadas, la forma de explotación y recomendaciones para eliminarlas o mitigar sus consecuencias.

Es necesario realizar indicadores de riesgo para tener una visión a futuro de las consecuencias que estos pueden traer.

Dependiendo del riesgo de cada control, se pueden utilizar indicadores que pueden usarse para tener generar alertas de forma temprana. Estos indicadores son: indicadores clave de riesgo, indicadores clave de rendimiento e indicadores clave de control. (Orozco, 2019)

1. Indicadores clave de riesgo (KRI): son los que cuantifican el perfil de riesgo. Se constituyen de acuerdo con el nivel de relevancia y representatividad de los indicadores de riesgo y de control. Por ejemplo, el volumen de operaciones, rotación de personal, número de veces que cae el sistema, etc (Orozco, 2019).

2. Indicadores clave de rendimiento o volumen (KPI): controlan la eficacia operativa y activan señales de alerta. Estas variables proporcionan información sobre eventos relacionados con pérdidas de tipo operacional y permiten cuantificar objetivos del desempeño estratégico de la organización (Orozco, 2019).

3. Indicadores clave de control (KCI): son aquellos que se encargan de medir la efectividad, tanto de diseño como de desempeño, de un control específico. Un deterioro en un KCI puede significar un aumento de la probabilidad de impacto de un riesgo (Orozco, 2019).

Etapa Actuar

Las etapas anteriores nos brindan una perspectiva de lo que conforma la red de automatización tanto en equipos como en programas, evalúan los diferentes riesgos que presentan al interconectarse con la red administrativa y definen controles para tratarlos y mitigar sus posibles efectos. Todas ellas presentan un enfoque preventivo, pero el riesgo no desaparece y se puede llegar a materializar y es ahí donde cobra importancia el concepto de plan de respuesta a incidentes (IRP por sus siglas en inglés).

El plan de respuesta a incidentes deja el enfoque preventivo de las fases anteriores y toma un enfoque correctivo. El riesgo está materializado y es necesario llevar el sistema de nuevo a su correcto funcionamiento para no afectar la operatividad de la compañía.

Dentro de los objetivos que tiene un plan de respuesta a incidentes están:

- Verificar que un incidente se ha producido: se enfoca en la detección del incidente. Se reconoce que un riesgo ha sido materializado y es necesario intervenir. Algunos de los incidentes que se pueden presentar son:
    - Robo o pérdida de datos confidenciales.

- Modificaciones no autorizadas o daños a los datos que comprometen su integridad.
- Daños o robos a los equipos o programas.
- Denegación de servicio.
- Uso indebido de los equipos o programas.
- Intento de acceso no autorizado.
- Cambios no autorizados de equipos, programas o su configuración.
- Reportes de comportamientos inusuales del sistema.
- Reporte de las alarmas de detección de intrusos.

- Reducir el impacto del incidente: se relaciona con la contención del incidente, evitar que afecte una parte mayor a la que se tiene detectada o sus efectos sean mayores. Los impactos de un incidente pueden llegar a ser no solo en la operatividad específica del proceso afectado, se deben tener en cuenta los posibles impactos frente a otros procesos o máquinas, las personas, la infraestructura y el medio ambiente. Un incidente podría llegar a afectar comunidades o el ecosistema pues estamos hablando de tecnología operativa que en el caso del café maneja gases, aguas de proceso y residuales, entre otros que podrían afectar las áreas circundantes de la organización.

  Algunos factores a tener en cuenta son:

  - ¿El incidente es real o percibido?
  - ¿El incidente aún está en curso?
  - ¿Qué datos, equipos y programas se ven amenazados y qué tan crítico es?

- ¿Cuál es el impacto que tiene o puede tener el incidente sobre el negocio?
- ¿A qué sistema, equipo, programa o proceso se dirige, dónde están ubicados físicamente y en la red?
- ¿El incidente se encuentra en el interior de la red de confianza?

- Mantener o restaurar la continuidad del negocio: este objetivo contiene la erradicación del incidente y la recuperación de la operatividad normal luego del mismo. Para ello entre otras actividades se deben asignar las prioridades a los incidentes con base en una definición de criterios propia y con ello los RTO y RPO.

El RTO (Recovery Time Objective) se refiere al tiempo objetivo en el que se debe recuperar el funcionamiento de un sistema (programa o equipo) luego de un incidente de seguridad.

El RPO (Recovery Point Objective) se refiere al punto en donde se hará la recuperación de datos luego de un incidente, es decir, cuantos datos se pueden perder cuando se presenta un incidente de seguridad.

- Determinar la forma en que el ataque se convirtió en incidente: en este objetivo se involucra el análisis forense. Mediante los registros del sistema y las huellas dejadas en el incidente se evalúa como los controles fueron vulnerados o si se hizo uso de una vulnerabilidad no detectada o nueva.
- Prevenir futuros ataques o incidentes: El resultado del objetivo anterior es el insumo para realizar de nuevo la evaluación y tratamiento de los riesgos detectados y con ello ajustar los controles existentes o crear nuevos.

Algunas de las actividades a realizar son:

- Cerrar un puerto o puertos en un equipo o programa.
- Apagar el sistema infectado hasta que se pueda volver a instalar.

- Generar un plan de capacitación para usuarios.
- Desactivar los servicios sin utilizar en el sistema afectado.

- Mejorar la seguridad y respuesta a incidentes: la mejora continua es lo que pretende este objetivo. La gestión de un incidente debe producir una mejora en la gestión de riesgos y al mismo tiempo en las capacidades de la organización para responder ante la materialización de un riesgo, adoptando nuevos procedimientos o mecanismos para ser más predictivos con las nuevas amenazas que se puedan identificar tempranamente.

  Se pueden hacer los siguientes cuestionamientos que ayudan a la mejora:

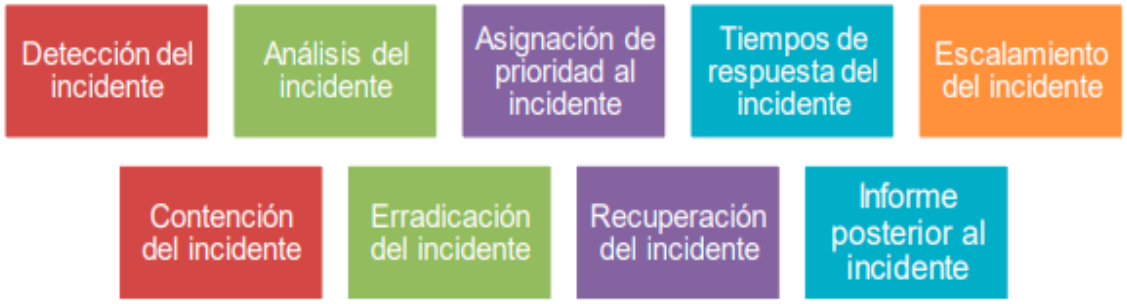
  - ¿Una política podría haber evitado la intrusión?
  - ¿Un procedimiento o política no se siguió, lo que permitió la intrusión?, ¿Qué se puede cambiar para que se siga en el futuro?
  - ¿Fue la respuesta a incidentes apropiada? ¿Cómo se puede mejorar?
  - ¿Las partes interesadas fueron informadas oportunamente?
  - ¿Los procedimientos de respuesta a incidentes fueron detallados y cubrieron toda la situación? ¿Cómo se pueden mejorar?
  - ¿Se han realizado cambios para evitar una situación de reincidencia?, ¿Están todos los sistemas actualizados, cerrados, contraseñas reforzadas, políticas comunicadas, etc.?
  - ¿Debería actualizarse alguna política de seguridad?
  - ¿Qué lecciones se aprendieron de la respuesta al incidente?

- Mantener información de la gestión de la situación y la respuesta: toda la información que se genera durante la detección y gestión de un incidente se debe

documentar pues es la base sobre la que se toman decisiones para mejorar el proceso de gestión del riesgo y respuesta ante incidentes futuros.

Figura 4

Componentes de un plan de respuesta a incidentes



Nota. Fuente: https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/7499/D%C3%ADaz_Ram%C3%ADrez_Milton_Fernando_2021.pdf?sequence=1

8. Análisis de Resultados

El trabajo proporciona recomendaciones específicas para la implementación de políticas de ciberseguridad para la conexión a las redes industriales en el contexto de las plantas de producción de café. Se destaca la importancia de adaptar las políticas a las necesidades y realidades específicas de cada empresa, y se sugiere el uso del ciclo PHVA de mejora continua de la ISO 27001 para garantizar que las políticas se revisen y ajusten constantemente.

La implementación de políticas de ciberseguridad para la conexión a las redes industriales siguiendo la metodología del ciclo PHVA con un enfoque en riesgos, propuesto en el trabajo, facilita la integración e interacción de estas con las normas adoptadas por Buencafé Liofilizado y DESCAFECOL. Adicionalmente brinda cumplimento a la guía de implementación de los estándares internacional BASC versión 6 de 2022 en lo que corresponde a ciberseguridad y tecnologías de la información.

En la etapa de planificación se sugiere realizar un inventario detallado de los equipos de automatización y programas SCADA utilizados en la empresa, con el fin de conocer los flujos de información y listar las amenazas relacionadas con la ciberseguridad.

Las etapas hacer y verificar proveen una evaluación de riesgos y determinan los controles para mitigarlos, además de crear las pruebas para determinar que los controles definidos son funcionales y adecuados.

La etapa actuar brinda planes de respuesta a incidentes, que serán ejecutados ante la materialización de algún riesgo a pesar de los controles definidos en las etapas anteriores, y su objetivo es brindar continuidad al negocio.

En general, se enfatiza la importancia de tomar medidas proactivas para proteger la información y los sistemas de automatización de posibles amenazas y vulnerabilidades, y se proporcionan recomendaciones específicas para lograr este objetivo.

9. Conclusiones

El uso de la metodología PHVA (Planear, Hacer, Verificar y Actuar) permite llevar un proceso estructurado para realizar una identificación de la infraestructura de equipos y servicios con las que cuenta una red de automatización y sus puntos de interconexión con la red administrativa en su fase de Planear; identificar las vulnerabilidades y valorar los riesgos que se presentan cuando se realiza interacción entre ambas redes al igual que los controles a implementar para mitigar esos riesgos en su fase de Hacer.

La etapa de Verificar nos permite crear estrategias que pongan a prueba los controles definidos y así saber si cumplen con su objetivo, son vigentes o si hay que reforzarlos o cambiarlos. La etapa de Actuar nos permite presentar los planes de respuesta a incidentes que se ejecutarán cuando alguno de los riesgos (identificados o no) se materialicen y así poder tener continuidad en el negocio.

Adicionalmente por ser un ciclo, cada iteración de las 4 fases permite una mejora continua de las políticas empresariales de ciberseguridad para la conexión de redes de automatización pues implica estar en revisión constante de los inventarios, controles y demás, siendo esta una estrategia dinámica y actualizable constantemente, respondiendo a los cambios de las amenazas nuevas.

Recomendaciones

Los resultados de este proyecto muestran que las políticas empresariales de ciberseguridad para la conexión de redes de automatización pueden definirse con base en una metodología estándar como el ciclo de Deming (PHVA), sin embargo, los resultados de la aplicación de la misma serán diferentes para cada empresa pues los inventarios de equipos y servicios, la identificación de vulnerabilidades y los controles son específicos a la empresa, su negocio y hasta su cultura organizacional. Las políticas de una empresa y hasta de una planta

de producción de café en específico no pueden ser copiadas y pegadas en otra pues muy probablemente estas no correspondan a la realidad de esta.

10. Referencias Bibliográficas

Alcaraz, Fernández, Román, Balástegui, & López. (2008). Gestión Segura de Redes SCADA. *NIC Labs Publication*, 20-25.

Federación Nacional de Cafeteros de Colombia. (s.f.). *Historia del Café de Colombia*. Obtenido de Café de Colombia: https://www.cafedecolombia.com/particulares/historia-del-cafe-de-colombia/

FORTINET. (s.f.). *FORTINET*. Obtenido de https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security

Geeta, & Kolin. (septiembre de 2021). *Science Direct.* Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S1874548221000251

ICONTEC. (07 de 2018). *Colección ICONTEC*. Obtenido de https://ecollection.icontec.org/normagrid.aspx

International Featured Standards. (s.f.). *IFS Food*. Obtenido de https://www.ifs-certification.com/index.php/es/standards/4132-ifs-food-standard-es

International Standard Organization. (Octubre de 2019). *ISO*. Obtenido de https://www.iso.org/standard/75106.html

Revista electroindustria. (Marzo de 2016). *Revista Electroindustria*. Obtenido de http://www.emb.cl/electroindustria/articulo.mvc?xid=2735&ni=sistemas-scada-la-evolucion-de-las-plataformas-de-monitoreo-y-control#:~:text=En%20la%20d%C3%A9cada%20de%20los,de%20monitorear%20y%20controlar%20equipamiento

World Basc Organization. (s.f.). *Certificación BASC.* Obtenido de https://www.wbasco.org/es/certificacion/certificacion-basc

sydle.com. (15 de 12 de 2021). Obtenido de https://www.sydle.com/es/blog/ciclo-pdca-61ba2a15876cf6271d556be9/

Ministerio de las Tecnologías de la Información y las Telecomunicaciones de Colombia. (2016, 03 15). *MINTIC.* From https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf - https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150516:Guia-de-gestion-de-riesgos

Nmap. (s.f.). *Nmap*. Obtenido de https://nmap.org/

Rapid 7. (s.f.). *Nexpose Vulnerability Scanner*. Obtenido de https://www.rapid7.com/products/nexpose/

SolarWinds. (s.f.). *SolarWinds*. Obtenido de https://www.solarwinds.com/es/

Tenable. (s.f.). *Tenable*. Obtenido de https://www.tenable.com

Wireshark. (s.f.). *Wireshark*. Obtenido de https://www.wireshark.org

Zone, R. (s.f.). Redes Zone. Obtenido de https://www.redeszone.net/tutoriales/seguridad/segmentacion-red-vlan-que-es/

Banco Santander. (s.f.). Obtenido de https://www.bancosantander.es/glosario/incidente-seguridad

COPADATA. (s.f.). COPADATA. Obtenido de https://www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que-es-scada/#:~:text=SCADA%20es%20el%20acr%C3%B3nimo%20de,registrar%20datos%20de%20sus%20operaciones.

Enredando con redes. (s.f.). Obtenido de https://enredandoconredes.com/2016/04/07/vulnerabilidades-en-sistemas-de-control-industrial-sci/

Zemsania Global Group. (s.f.). Obtenido de https://zemsaniaglobalgroup.com/category/actualidad-zemsania/

11. Anexo 1 - Definiciones

OT: es un término para referirse al conjunto de tecnologías que se utilizan en los procesos industriales y también en la gestión de infraestructuras, destinadas a realizar la operación de estas. (Zemsania Global Group, s.f.)

SCADA: es el acrónimo de Supervisory Control and Data Acquisition (supervisión, control y adquisición de datos), término que describe las funciones básicas de un sistema SCADA. Las empresas usan los sistemas SCADA para controlar los equipos de sus centros y recopilar y registrar datos de sus operaciones (COPADATA, s.f.).

Vulnerabilidad: Son aquellas debilidades en los sistemas de información, procesos, implementaciones o controles sobre sistemas, que pueden ser explotadas por una amenaza. (Enredando con redes, s.f.)

Riesgo: Propiedades de una organización, procesos de negocio, arquitectura, y sistemas de información que puedan favorecer en la probabilidad de que un evento generado por una amenaza pueda surtir efecto. (Enredando con redes, s.f.)

Incidente de seguridad: Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella. (Banco Santander, s.f.)

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co