Universidad Abierta Interamericana
2023

Diseñar el plan de ciberseguridad basado en la Norma IEC 62443

Tutoría técnica: Ing. Romero, Raúl Oscar

Profesores de Trabajo Final:

Dra. Samela, Marcela

Mg. Ugarte, Carlos Alberto

Alumno: Pobeda, Sebastián

Trabajo Final de Carrera presentado para obtener el título de
Lic. en Gestión de Tecnología informática

Diciembre, 2023

Resumen

El presente trabajo es una propuesta de intervención en el campo profesional, el objetivo principal es analizar el estado actual de la infraestructura, políticas y procedimientos del entorno industrial de la planta de grasos y margarinas de la empresa “CALSA” (Cía. Argentina de Levaduras S.A.I.C), la cual desarrolla su actividad comercial en el sector alimenticio en la industria de la panificación.

Se realizó el relevamiento de la infraestructura instalada, equipamiento existente, políticas y procedimientos implementados y en vigencia, el análisis de los hallazgos permitió completar el diagnostico, identificar la postura respecto a la ciberseguridad y los riesgos inherentes.

El resultado alcanzado ha sido el diseño de un plan de ciberseguridad, basándose en la Norma IEC 62443, que le permitirá adoptar a la empresa CALSA (Cía. Argentina de Levaduras S.A.I.C) estándares internacionales, generar nuevas políticas, procedimientos, reducir las vulnerabilidades y riesgos identificados logrando que la infraestructura del entorno industrial sea más segura, incluyendo un programa de entrenamiento para todos los integrantes de los equipos industriales y de IT.

Palabras clave: CALSA, ciberseguridad, ICS, IEC 62443, industria 4.0, redes industriales, sistemas SCADA, vulnerabilidades

Abstract

The present work is a proposal for intervention in the professional field, the main objective is to analyze the current state of the infrastructure, policies, and procedures of the industrial environment of the fat and margarines plant of the company "CALSA" (Cía. Argentina de Levaduras S.A.I.C), which develops its commercial activity in the food sector in the bakery industry.

A survey of the installed infrastructure, existing equipment, policies and procedures implemented and in force will be carried out, analyzing the findings will allow the diagnosis to be completed, identifying the posture regarding cybersecurity and the associated risks.

The result achieved has been the design of a cybersecurity plan, based on the IEC 62443 Standard, which will allow the company CALSA (Cía. Argentina de Levaduras S.A.I.C) to adopt international standards, generate new policies, procedures and reduce vulnerabilities and risks. identified, making the infrastructure of the industrial environment safer, including a training program for all members of the industrial and IT teams.

Keywords: CALSA, Cybersecurity, ICS, IEC 62443, industrial networks, industry 4.0, SCADA systems, vulnerabilities

Dedicatoria

En primer lugar, quiero expresar mi eterno agradecimiento a Valeria, Catalina y Facundo por su incondicional apoyo durante todo el proceso de elaboración del presente trabajo y todos los años de cursada, una mención especial para Valeria que se hizo cargo de muchas cosas en mis momentos de estudio, siempre pensando en positivo.

A mi familia y amigos, que también me dieron todo su apoyo y me alentaron en los momentos difíciles.

Agradecimiento o Reconocimientos

A la empresa CALSA, que me dio la oportunidad de realizar el Trabajo Final de Carrera basada en una necesidad de la empresa.

Quiero agradecer a Sergio Vazquez, Hernán Bertotto, Silvio Szostak y Alejandro Difino por su orientación y apoyo constante.

Agradezco a la Universidad Abierta Interamericana (UAI), a sus autoridades, cuerpo docente y no docente.

A Oscar Romero mi tutor, por acompañarme en este momento, por sus consejos, apoyo e insistencia en los momentos difíciles.

Finalmente quiero agradecerle a Marcela Samela y Carlos Ugarte por su guía en la formulación de este trabajo.

Índice General

Índice de figuras

Índice de tablas

Capítulo I

1.1. Identificación del problema

El avance de las tecnologías le permitió al mundo evolucionar como sociedad, estos nuevos avances tecnológicos en la historia de la humanidad se conocen como la revolución industrial, estos procesos no se consiguieron de forma inmediata, sino que se desarrollaron lentamente, teniendo como sus principales ejes el desarrollo social y la economía apoyándose en la ciencia y la tecnología.

El origen de la revolución industrial fue en Inglaterra en el siglo XVIII entre los años 1750 al 1780. El profesor David S. Landes se refiere a la revolución industrial al complejo de innovaciones tecnológicas que, al sustituir la habilidad humana por las maquinas provoca la transformación de la producción artesanal a la fabril, produciendo el nacimiento de la economía moderna. (Landes, 1979, pág. 15). La aparición de la máquina de vapor, el tren, el telar mecánico, el hierro como el insumo más determinante y el carbón como la principal fuente de energía fueron los principales avances. El desarrollo de la minería a través del carbón se transformó rápidamente en una de las principales fuentes de energía, permitió que las industrias estén ubicadas en las cercanías de las cuencas carboníferas, al aumentar el nivel de industrialización, fue mayor la necesidad de extracción de carbón, esto incrementó la producción, ocasionando un crecimiento de la oferta y abaratando el costo, e impulsando el desarrollo de la industria metalúrgica. La industria textil, se vio beneficiada con la introducción de máquinas como la lanzadera volante, la hiladora y el telar mecánico, estos avances tecnológicos contribuyeron en reducir los tiempos y escalar la producción. Otra de las actividades que se expandió fue la siderurgia, que, a través del hierro y el acero, permitió la producción de trenes, rieles y herramientas, el transporte se vio beneficiado por este avance tecnológico que junto con las máquinas de vapor permitieron impulsar la adopción de los trenes y barcos, expandiendo el comercio de forma significativa. Estas innovaciones tecnológicas también produjeron grandes cambios sociales y desigualdad entre los obreros y los dueños de las fábricas, las poblaciones rurales se trasladaron a las ciudades en donde estaban instaladas las fábricas en busca de oportunidades, incrementando la cantidad de habitantes en estas zonas, que no estaban preparadas para recibirlos, generando pobreza, malas condiciones habitacionales, suciedad, etc. Debido a los abusos laborales que los dueños de las fábricas ejercían sobre sus empleados, es que el gobierno de Inglaterra sanciona nuevas leyes que permiten proteger a las mujeres y niños, respecto a la cantidad de horas laborales y actividades que podían desarrollar. El resto de los países de Europa y Estados Unidos iniciaron su proceso

de industrialización utilizando los avances realizados por Inglaterra, tanto en la tecnología como en mano de obra calificada que era contratada para la capacitación en el uso de las máquinas y motores. (Chaves Palacios, 2004)

La segunda revolución industrial se produjo a mediados del siglo XIX, el principal avance tecnológico fue la electricidad, y su aplicación en las industrias, hogares y transporte. A diferencia de la primer revolución industrial esta tuvo una expansión mayor territorialmente hablando, en Europa del Este, Estados Unidos y Japón. Se incorporan conceptos como la producción en serie, en donde aparecen las primeras líneas de montajes, la división de las tareas y la toma de tiempos, con el principal objetivo de aumentar la productividad. Lo anteriormente mencionado le permitió a la industria automotriz crecer rápidamente mejorando los tiempos de producción de cada vehículo y reduciendo el precio de venta. El desarrollo de los motores a combustión fue revolucionario innovando en otras fuentes de energías, como el petróleo y la electricidad. La aparición del teléfono y la radio impulsó el crecimiento de la industria de las telecomunicaciones. Los avances tecnológicos introducidos por la segunda revolución industrial tuvieron como consecuencias, el aumento de la producción, desarrollo del comercio, la creación y crecimiento de los centros urbanos, promovió la competencia entre las empresas, como también el desempleo. Todos estos hechos también acarrearon que los obreros sigan luchando por sus derechos, creando sindicatos que les permitieran organizarse para enfrentar a los capitalistas, mejorar las condiciones de vida, y controlar la explotación laboral.

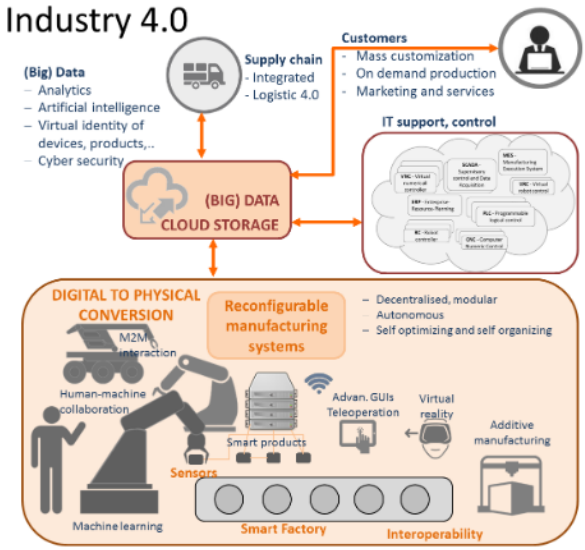
La tercera revolución industrial o revolución digital, se apoya en tres pilares fundamentales que deben ser desarrollados de forma simultánea e integrados entre ellos, estos pilares son: las energías renovables, tecnologías de almacenamiento y las redes eléctricas inteligentes. Las diferentes formas de energías renovables: solar, eólica, hidroeléctrica, geotérmica, y biomasa, mientras estas formas de energías representan un pequeño porcentaje de la energía global, los gobiernos avanzan en la implementación de normativas y regulaciones para promover el uso de las energías renovables y generar incentivos para la transición de los vehículos que utilizan combustibles fósiles hacia las energías limpias, ayudando a las organizaciones y gobiernos a reducir la huella de carbono y lograr la soberanía energética. Para poder potenciar el primer pilar de las energías renovables fue determinante el desarrollo del segundo pilar que es la tecnología de almacenamiento, la clave fue poder reducir los costos asociados a este concepto, esto implico destinar muchos recursos a la investigación y desarrollo de métodos basados en el hidrogeno, ya que es considerado el medio universal para almacenar todas las expresiones de energías renovables. El ultimo pilar fue invertir en tecnología para el

crecimiento de la red eléctrica inteligente, permitiéndole a las empresas y los hogares que sean productores de energía eléctrica, pudiendo comprar y vender electricidad ecológica mediante un sistema de red eléctrica inteligente, continental e interactivo que censa los consumos y permite mediante la información que tiene de la red, redireccionar en base a los picos de consumos. (Rifkin, 2011).

Desde 1950 en adelante el auge de la informática y las telecomunicaciones, permitió el desarrollo de tecnologías y conocimiento, estos avances también ocasionaron que se deban tener en cuenta otros tipos de mecanismos de control. La revolución industrial 4.0 o industria 4.0 comenzó en Alemania, conceptualmente es la interrelación de los sistemas informáticos, la robótica, los procesos industriales, la convergencia entre lo físico y lo virtual, explotando las nuevas tecnologías. Esta interconexión entre dispositivos y tecnologías permite ir en la búsqueda del concepto de fábricas inteligentes, incorporando tecnologías como Big Data, Cloud Computing, IoT de sus siglas en inglés "Internet of Things" y Ciber Seguridad, entre otras, para que este camino sea exitoso, seguro y confiable se requerirá de estrategias de ciberseguridad y herramientas que permitan preservar los activos clasificados como críticos para una organización, ya que estos son los que le permitirán lograr de forma exitosa sus objetivos comerciales, ser competitivos, garantizar la continuidad del negocio, reducir los costos de producción, logísticos y de aseguramiento de la calidad, además de generar información para la toma de decisiones en tiempo real basada en hechos pasados (Rojko, 2017).

Figura 1

Industria 4.0 y sus componentes

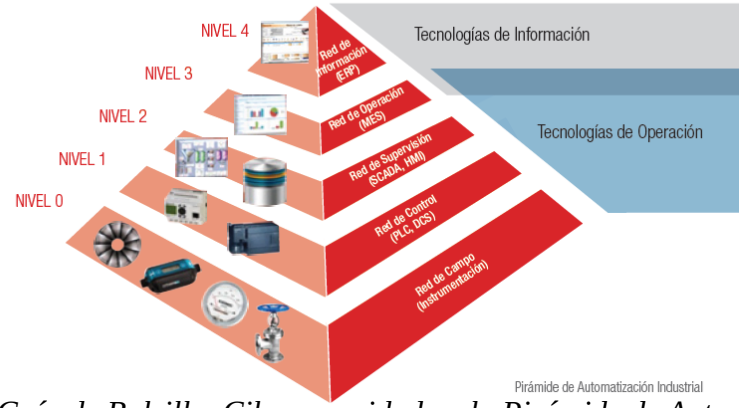


Nota. Extraído de Industry 4.0 Concept: Background and Overview (Rojko, 2017).

La Figura 2 nos ayuda a entender como está conformada la pirámide de automatización en sistemas de producción, en donde el software tiene una importancia relevante en la operación de las industrias 4.0. En la capa superior llamada Enterprise business, las organizaciones tienen implementados sistemas de información llamados ERP, de sus siglas en ingles "Enterprise Resource Planning", este tipo de sistemas permite a las organizaciones cubrir todos los procesos de negocios, como ser ventas, producción, abastecimiento, etc. La segunda capa es identificada como Red de Operación, también conocida como MES, de sus siglas en ingles "Manufacturing Execution System", en esta capa es donde se comunican los sistemas industriales con los sistemas de información ERP, de sus siglas en ingles "Enterprise Resource Planning", realizando la programación de producción, de recursos, materias primas, paradas de plantas para su mantenimiento correctivo y preventivo, y reportes de producción. La tercera capa es conocida como Red de Supervisión, aquí intervienen los sistemas SCADA, de sus siglas en ingles "Supervisory Control and Data Acquisition", son sistemas que permiten supervisar y controlar la operación, recolectando datos desde sensores. (Alcaraz, et al, 2008). La cuarta capa es llamada Red de Control en donde los PLC, de sus siglas en inglés "Programmable Logic Controllers" son los principales actores, los PLC son controladores que carecen de potencia de cómputo, envían y reciben información del estado del equipamiento de la última capa llamada Red de Campo, en tiempo real, están conectados en la LAN, de sus siglas en ingles "Local Area Network" y se integran con el piso de fábrica, en donde los sensores y actuadores recolectan la información y la envían a la capa superior.

Figura 2

Pirámide de Automatización Industrial



Nota. Extraído de Guía de Bolsillo. Ciberseguridad en la Pirámide de Automatización Industrial (Centro de Ciberseguridad Industrial, s.f.).

Alemania desarrollo para la industria 4.0 una arquitectura de referencia llamada RAMI 4.0 de sus siglas en inglés “Reference architecture model industry 4.0” (Meyer, 2017) en donde la norma IEC 62443 es la base para que los entornos industriales operen de forma segura. Basarse en arquitecturas y normas de referencia, ayudan en la estandarización de los procesos. La capa de Activos de sus siglas en inglés “Asset”, incluye componentes físicos como robots, cintas transportadoras, PLC de sus siglas en inglés “Programmable Logic Controllers”, documentos, archivos, software e ideas. En la capa de Integración de sus siglas en inglés “Integration” podemos encontrar la información en un formato procesable digitalmente, incluye sensores, dispositivos HMI de sus siglas en inglés “Human Machine Interface” y control de procesos. La capa de Comunicación nos permite estandarizar las comunicaciones utilizando formatos de datos y protocolos predefinidos. En la capa de Información se procesan e integran los datos transformándolos en información utilizable. La capa Funcional es la responsable de documentar las descripciones funcionales de los procesos o reglas de negocio que deben estar contempladas en el modelo. Finalmente, la capa de Negocios incluye el mapeo de los procesos y el modelo de negocio. (Rojko, 2017).

Figura 3

Modelo Arquitectónico de Referencia para la Industria 4.0 (RAMI 4.0)

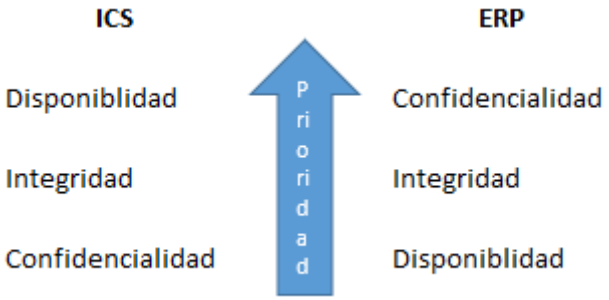
Nota. Extraído de Serie Smart OT Nro. 3, Actores de la “Smart OT” (Centro de Ciberseguridad Industrial)

Las redes industriales inteligentes amplían las capacidades de las redes industriales tradicionales respecto a las tecnologías de automatización para enfocarse en la recolección,

análisis y explotación de datos, generando información confiable que le permita a las organizaciones mejorar los proceso productivos y aumentar su rentabilidad.

Figura 4

Comparativa de Prioridades entre ICS y ERP

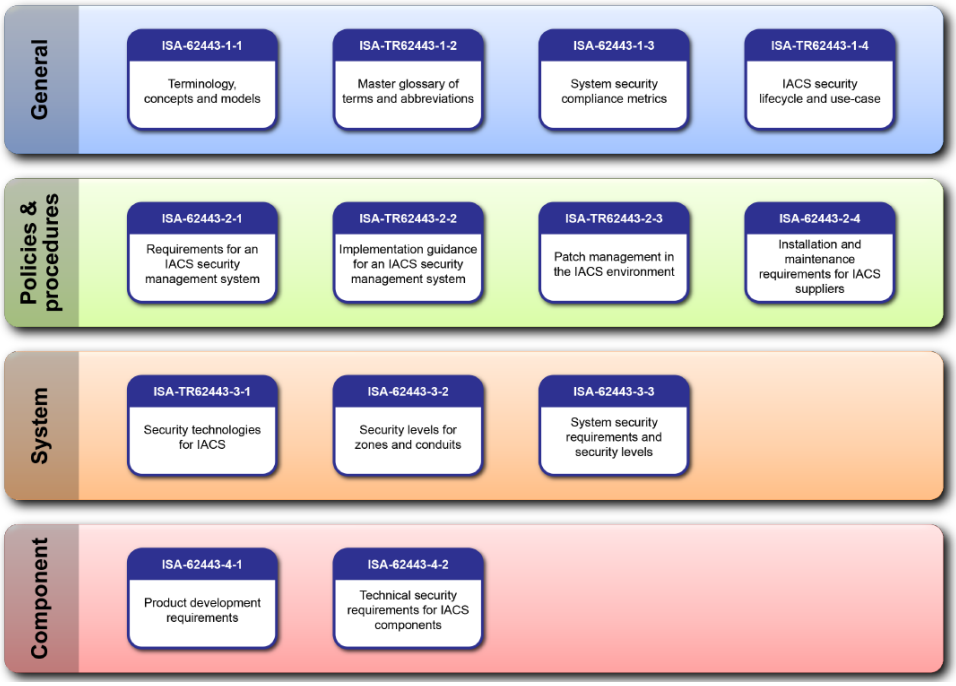


Nota. De elaboración propia. Comparativa de Prioridades entre ICS y ERP.

La falta de programas de ciberseguridad genera que los aspectos básicos para la continuidad del negocio no sean visibles dentro de las organizaciones, impidiendo evaluar o cuantificar los riesgos e impactos asociados. La seguridad de la información se ha centrado en lograr tres objetivos, la confidencialidad, la integridad y la disponibilidad, que se abrevian con el acrónimo CIA. La integridad es la propiedad de proteger la exactitud y completitud de los activos, evitando la corrupción de datos, los controles de integridad deben ser incorporados dentro de los procedimientos, reduciendo la probabilidad de cometer errores. Sobre la disponibilidad podemos mencionar que es la propiedad de ser accesible y utilizable. Respecto a la confidencialidad es la característica que nos asegura que la información será accesible solo por las personas autorizadas. (ISO/IEC 27000:2018, 2018). La estrategia en seguridad de la información en un ERP, de sus siglas en inglés “Enterprise Resource Planning” puede centrarse en la confidencialidad y los controles de acceso necesarios para lograrlo mientras que la integridad puede ser la segunda prioridad y la disponibilidad como la más baja. En los Sistemas de Control Industrial (ICS), de sus siglas en inglés “Industrial Control System”, la prioridad suele ser diferente, la seguridad en estos sistemas se ocupa de mantener la disponibilidad de todos los componentes. Por lo tanto, la integridad tiende a ser la segunda en importancia. Por último, la confidencialidad es de menor relevancia, porque los datos solos sin ser analizados dentro de un contexto no tienen valor.

Figura 5

Documentos IEC 62443



Nota. Extraído de Deploying CIP Security within a Converged Plantwide Ethernet Architecture. Design Guide (Cisco Systems)

La Comisión Electrotécnica Internacional (IEC) de sus siglas en inglés “International Electronic Commission”, es una organización mundial de normalización que abarca a todos los comités electrotécnicos internacionales, el objeto es promover la cooperación internacional respecto a la normalización en los campos eléctrico y electrónico. Dicha normalización consiste en la publicación de normas, especificaciones técnicas e informes, todos los organismos internacionales, gubernamentales y no gubernamentales que se estén asociados a el IEC de sus siglas en inglés “International Electronic Commission” pueden participar, además colabora con la Organización Internacional de Normalización (ISO) de sus siglas en inglés “International Standar Organization”. La normativa IEC de sus siglas en inglés “International Electronic Commission” 62443 (ISA, s.f.) es un conjunto de especificaciones técnicas basados en los conceptos definidos por la Norma ISA99 (ISA, s.f.), que son utilizados en los entornos industriales como guías para establecer las recomendaciones de las mejores prácticas y permitiendo incrementar la seguridad de los sistemas de control industriales frente a ciber ataques. El término "seguridad" se considera como la prevención del acceso o la penetración ilegal o no deseada, la interferencia intencional o no, acceso inapropiado a la información confidencial dentro de los Sistemas de Control Industrial (ICS). La ciberseguridad es el

enfoque particular de esta especificación técnica, en donde se incluyen computadoras, redes, sistemas operativos, aplicaciones y otros componentes configurables dentro de los sistemas. (IEC/TS 62443, 2009)

Como se observa en la Figura 5, el estándar se ha dividido en cuatro niveles que se explican a continuación. El primer nivel se llama General e incluye cuatro documentos en donde se definen los conceptos básicos, modelos, glosarios y métricas, que forman la normativa y pueden ser utilizados como base para diseñar un programa de seguridad.

En la Tabla 1 podemos encontrar el segundo nivel, llamado Management System (Policies & Procedures) describe las políticas, procedimientos que deben ser usados para implementar un sistema de gestión de ciberseguridad, las guías de operación, como gestionar las vulnerabilidades y los requisitos que deben cumplir los proveedores.

Tabla 1

IEC 62443 – Management System (Policies & Procedures)

Niveles	62443-2-1	62443-2-2	62443-2-3	62443-2-4
Management System (Policies & Procedures)	Requisitos para definir e implementar un sistema de gestión de ciberseguridad.	Guías de operación.	Gestión de vulnerabilidades.	Requisitos que deberán cumplir los proveedores

Nota. De elaboración personal basado en la IEC 62443

La Tabla 2, se llama System Requeriments, está compuesta de tres documentos, en donde propone las mejores prácticas para la implementación de forma segura de los sistemas en entornos industriales.

Tabla 2

IEC 62443 – System Requeriments

Niveles	62443-3-1	62443-3-2	62443-3-3
System Requeriments	Describe la aplicación de diferentes tecnologías de seguridad en un sistema industrial.	Explica la forma de hacer la evaluación de riesgos y el diseño en sistemas industriales.	Describe las bases de los requerimientos y los niveles de seguridad

Nota. De elaboración personal basado en la IEC 62443

Por último, en la Tabla 3 está el cuarto nivel que se llama Component, incluye dos documentos y especifica los requerimientos que deben cumplir los fabricantes de dispositivos industriales para ajustarse a la norma.

Tabla 3

IEC 62443 – Component

Niveles	62443-4-1	62443-4-2
Component	Requisitos que se aplican en el desarrollo de productos.	Especifica como mapear los requisitos del sistema, con los subsistemas y componentes de bajo nivel.

Nota. De elaboración personal basado en la IEC 62443

1.2. Justificación

Los sistemas de control y automatización industrial (IACS) de sus siglas en inglés "Industrial Automation and Control System" operan en entornos muy complejos y variados. Es cada vez más frecuente que los sistemas ERP, de sus siglas en ingles "Enterprise Resource Planning", compartan e intercambien información entre los sistemas de automatización comercial e industrial (IACS) de sus siglas en inglés "Industrial Automation and Control System". La pérdida información crítica y confidencial, no son las únicas consecuencias de una brecha de seguridad, la pérdida de vidas, producción, el daño ambiental, la violación de las leyes locales, la reputación, la continuidad del negocio y el compromiso de la seguridad operativa son consecuencias mucho más graves. Las amenazas externas no son las únicas preocupaciones, también existen las amenazas de origen interno, en este grupo podemos encontrar a miembros de la organización que pueden tener actitudes mal intencionadas o no y que representen un grave riesgo para la seguridad.

Tabla 4

Diferencias entre la Seguridad IT y los Entornos Industriales

Seguridad	Sistemas IT	ICS
Antivirus (AV)	Implementado	Imposible de implementar
EDR	Implementado	Imposible de implementar
XDR	Implementado	Imposible de implementar
Ciclo de Vida	3 a 5 años	5 a 20 años
Concientización	Buena	Mala
Gestión de Actualizaciones	Buena	Mala/Escaso
Gestión del cambio	Regular/Programado	Mala/Escaso
Revisión de Logs	Frecuente	Escaso
Dependiente del Tiempo	Aceptable	Critico
Disponibilidad	Demoras aceptadas	7x24
Concientización en Seguridad	Buena	Mala
Test de Seguridad	Frecuente	Imposible de implementar
Test de los ambientes	Frecuente	Imposible de implementar

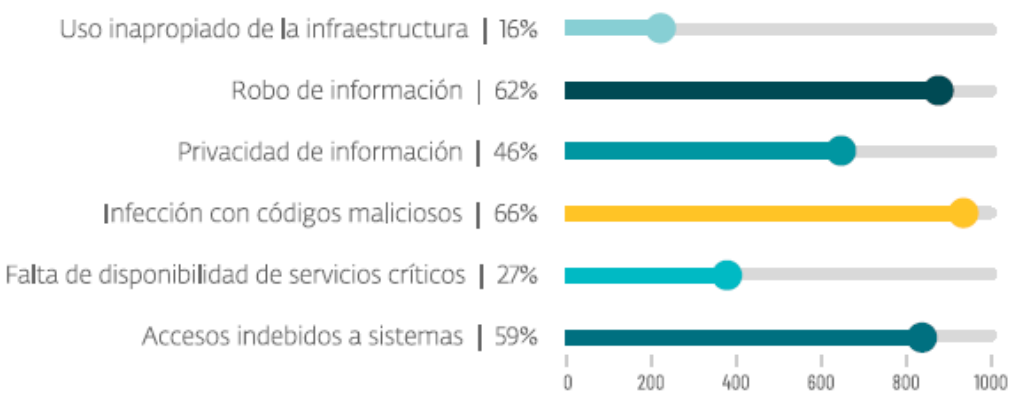
Nota. De producción propia. Diferencias entre la Seguridad IT y los Entornos Industriales.

Como podemos apreciar según la información que nos proporciona la Tabla 4, las diferencias entre la seguridad aplicada en entornos controlados por IT de las siglas en inglés de “Information Technologies” y los entornos industriales muestran claramente el desfasaje de madurez tanto en las tecnologías utilizadas, los sistemas y los procedimientos.

Según los dos últimos informes de Eset para Latinoamérica (Eset, 2021) (Eset, 2022), basados en información recolectada entre más de 1000 empresas se logró identificar los comportamientos y dificultades respecto a la seguridad que las organizaciones en Latinoamérica deben enfrentar a diario, en donde el malware o código malicioso se identifica como la principal preocupación de los responsables de IT, siendo estos cada vez más agresivos y utilizando la extorsión económica para restablecer el estado original de la información. Brasil, México y Argentina son los países más afectados en la región.

Figura 6

Principales Preocupaciones de las Empresas de América Latina en Temas de Seguridad.

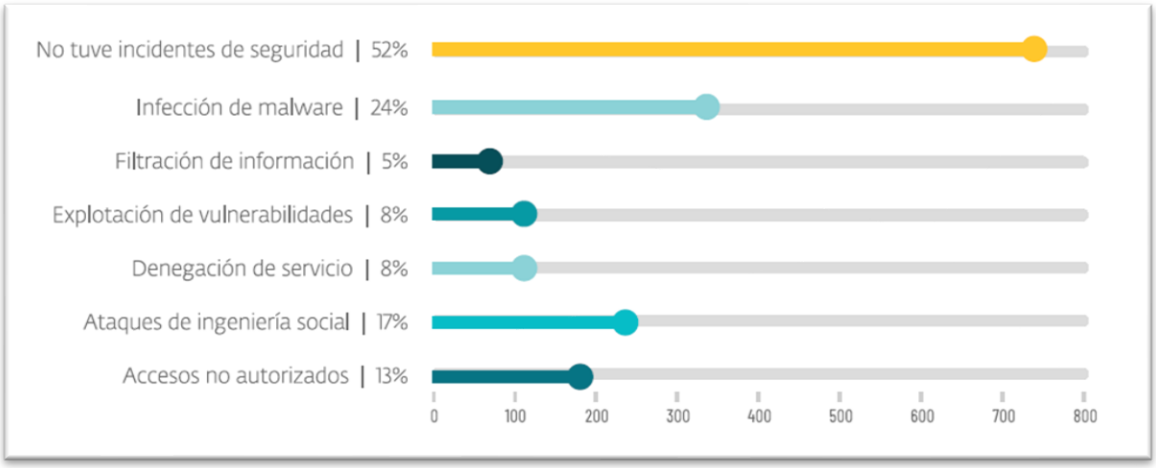


Nota. Información extraída Eset Segurity Report Latino América 2022 (Eset, 2022).

Las principales preocupaciones respecto a la seguridad de las organización son la infección de código malicioso (66%), el robo de información (62%) y el acceso indebido a los sistemas (59%). A continuación, en la Figura 8, se detallan los incidentes de seguridad reportados en el 2022, estos casos están altamente relacionados con las herramientas tecnológicas de detección y de gestión que posean las organizaciones, además de la complejidad de los ataques recibidos.

Figura 7

Incidentes de Seguridad de la Información en las empresas de Latinoamérica.



Nota. Incidentes de Seguridad de la Información en las Empresas de Latinoamérica (Eset, 2022)

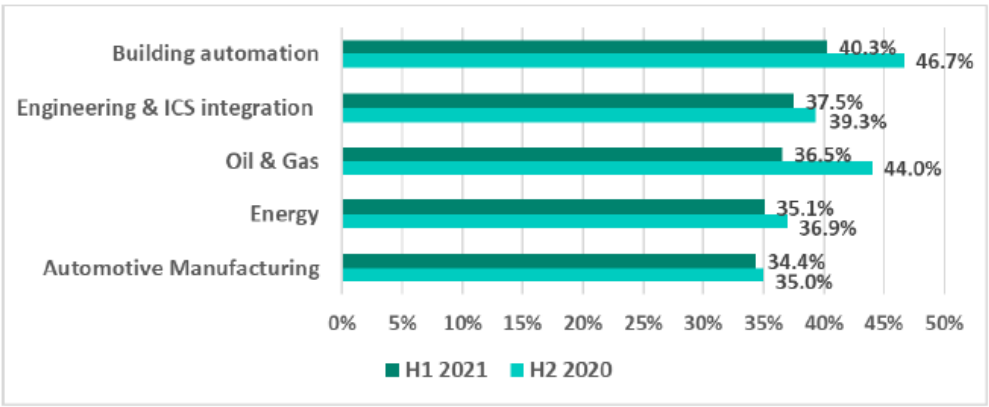
Los datos que expuestos en la Figura 8 nos permite analizar que el malware (24%), los ataques de ingeniería social (17%) y los accesos no autorizados (13%) son los 3 tipos de ataques

más frecuentes. El incremento de los ciberataques como negocio concluye que cada año haya más demanda y dinero en los mercados clandestinos, utilizando las cripto monedas como la principal forma de pago debido a que es imposible rastrear el destino final de esos fondos y la amenaza de la filtración de los datos en los casos que las víctimas no paguen la extorsión. De acuerdo con los datos informados por la oficina de Control de Crímenes Financieros (FinCEN) de los Estados Unidos, entre enero y junio del 2022 el promedio mensual de transacciones sospechosas en Bitcoin relacionadas con el ransomware es de 66.4 millones de dólares. El modelo de negocio de los ciber delincuentes se expandió rápidamente y ofrecen el rasonware como un servicios (Raas) de sus siglas en inglés “Rasonware as a Service” (Eset, 2022).

De acuerdo con los informes “Theat landscape for industrial automation System” de Kapersky en 2019 y 2021 las principales industrias que sufrieron ataques en sus Sistemas de Control Industrial fueron las de automatización, ingeniería, petróleo, energía y automotrices. (Kapersky, 2019) (Kaspersky, 2021).

Figura 8

Comparativa entre las industrias más atacadas entre el 2020 y 2021

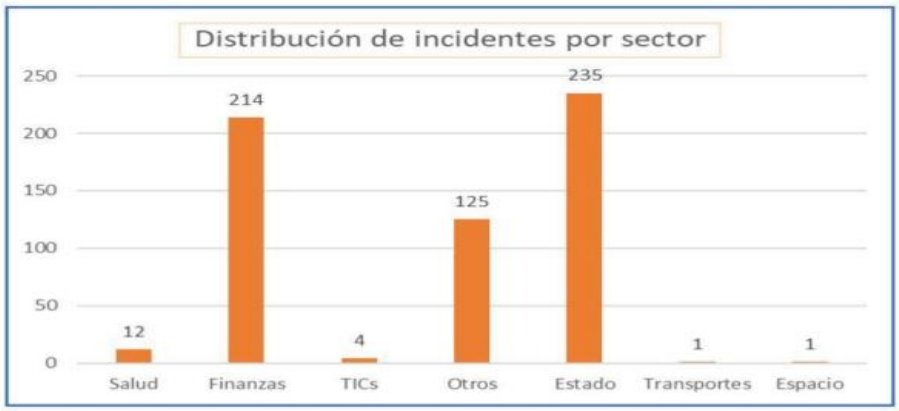


Nota. Extraído del Informe Theat Landscape for Industrial Automation System (Kaspersky, 2021)

El informe indica que Europa del este y principalmente Bielorusia, Ucrania y Rusia son los países que lideran el raking desde donde se originan estos ataques, en donde internet, el uso de medio removible y el correo electrónicos son los principales orígenes de las amenazas.

Figura 9

Distribución Anual de Incidentes por Sector



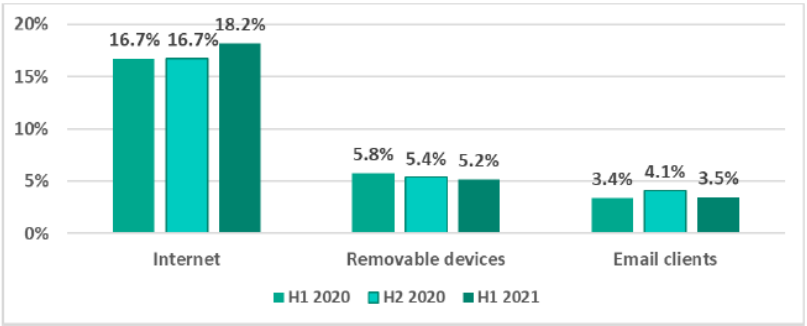
Nota. Extraído del Informe del Cert.ar 2022 (Informe anual del CERT.ar, 2022)

La Figura 10 proviene del informe publicado por el Cert (Centro Nacional de Respuesta a Incidentes Informáticos) para el año 2022, en donde podemos visualizar que los sectores más afectados por ciber ataque fueron Finanzas, Estado, Salud, Otros, Transportes, Espacio y el de las Tecnologías de la Información y las Comunicaciones (TICs), siendo el Estado y Finanzas los sectores que más ataques recibieron (%70) (Informe anual del CERT.ar, 2022).

Durante la primer mitad del 2021 el porcentaje de ataques a redes industriales fue del 33,8%, en donde el uso de internet, medios USB (pen drives y discos externos) y del correo electrónico, fueron los principales vectores de ataque utilizados. La Figura 11 representa los principales orígenes de las amenazas entre el período comprendido entre los años 2020 y 2021.

Figura 10

Principales Orígenes de las Amenazas

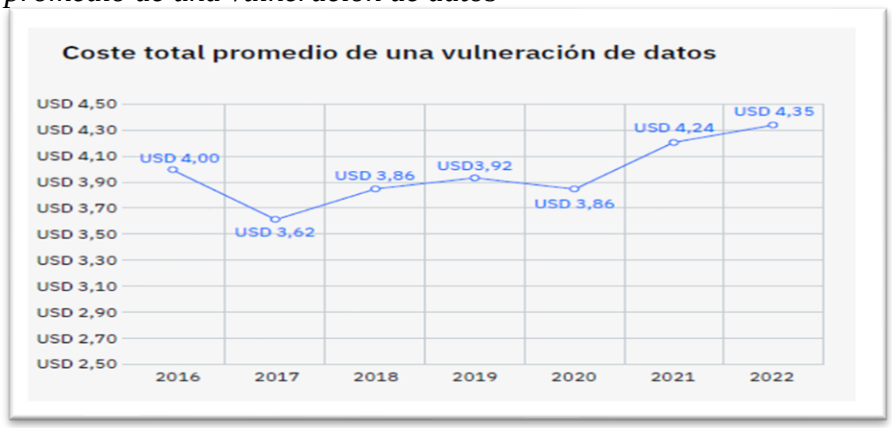


Nota. Extraído del Eset Security Report para Latino América 2021 (Eset, 2021).

Los hallazgos obtenidos en el informe de IBM Security (Security, IBM, 2022) nos indican que durante el año 2022 el costo promedio de la vulneración de los datos para las organizaciones tuvo un incremento del 2,6% respecto al año anterior representando 4,35 millones de dólares, este mismo informe nos indica que el costo promedio de un ataque de rasonware para las organizaciones es de 4,54 millones de dólares, representando un 41% de crecimiento respecto al año anterior.

Figura 11

Costo total promedio de una vulneración de datos

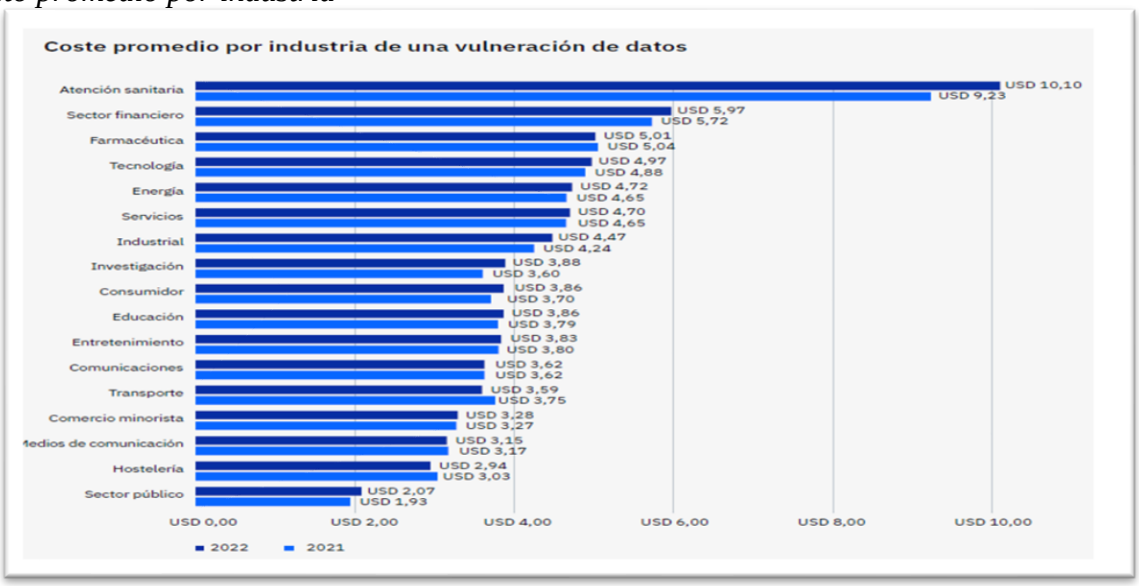


Nota. Extraído del informe IBM Security (Security, IBM, 2022).

El costo promedio por industria de una vulnerabilidad de datos de los años 2021 y 2022, según el informe de IBM Security (Security, IBM, 2022) esta medido en millones de dólares y nos indica que respecto al año 2021 se incrementó un 9,4%.

Figura 12

Costo promedio por industria

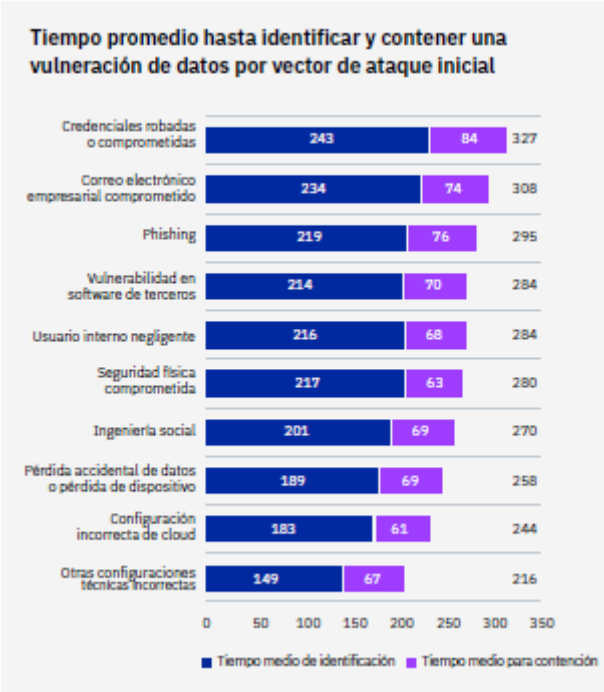


Nota. Extraído del informe IBM Security (Security, IBM, 2022).

Actualmente las organizaciones destinan mucho dinero, recursos y esfuerzo en la detección, notificación y remediación, con el principal objetivo de disminuir los millones de dólares que pierden luego de un ciberataque, en el 2022 el ciclo de vida de las vulnerabilidades se redujo en un 3,5% respecto al año anterior, por ciclo de vida de una vulnerabilidad nos referimos al tiempo que pasa desde que una organización identifica y contiene una vulnerabilidad, este porcentaje expresado en días es 207 para identificar la vulnerabilidad y 70 días para contenerla. A continuación, podemos observar en la Figura 14, los principales vectores de ataque y el tiempo promedio en identificar y contener la brecha de seguridad (Security, IBM, 2022).

Figura 13

Tiempo Promedio hasta Identificar y Contener una Vulneración de datos por vector de Ataque Inicial.

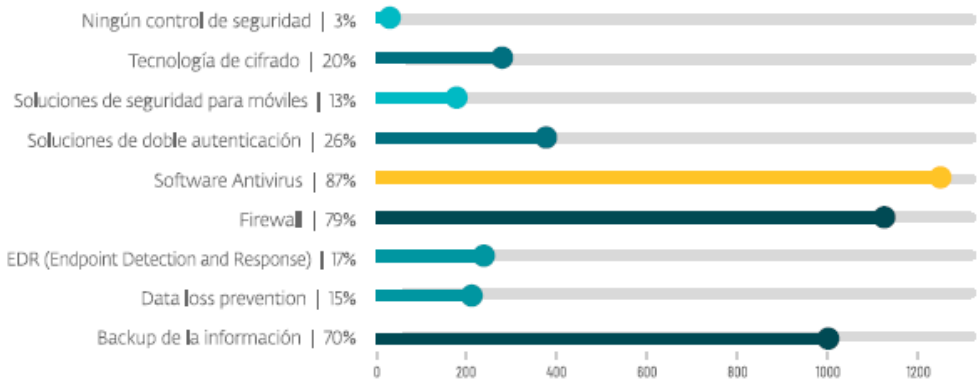


Nota. Imagen extraída de IBM Security (Security, IBM, 2022).

Consideramos que los entornos industriales (ICS) se deben adaptar a los continuos retos y amenazas que actualmente presenta la ciberseguridad, adoptando las mejores prácticas y los estándares de la industria, utilizando las herramientas tecnológicas les permitirá a las organizaciones defender sus infraestructuras críticas de las amenazas existentes y futuras, pudiendo adoptar una mejor postura de ciber seguridad, reducir el tiempo y los costos asociados a los incidentes de seguridad.

Figura 14

Soluciones de seguridad más utilizadas por las empresas en América Latina



Nota. Imagen extraída de Security Report LatinoAmérica 2022 (Eset, 2022).

El informe de Eset para Latinoamérica (Eset, 2022) expone cuáles son las principales soluciones de seguridad más utilizadas por las empresas en América Latina, un 3% no posee ningún tipo de control de seguridad, un 87% utiliza algún tipo de software antivirus, que por el nivel de avance tecnológico y versatilidad de las nuevas tendencias de ataque con solo tener un antivirus no alcanza, hoy las mejores prácticas de la industria recomiendan utilizar las soluciones de EDR/XDR, de sus siglas en ingles “EndPoint Detection and Response/Extended Detection and Response”, también se puede observar una muy baja adopción tecnologías de cifrado para las computadoras, protección de dispositivos móviles mediante soluciones MDM, de sus siglas en ingles “Mobile Device Management” y doble factor de autenticación, 2FA, de sus siglas en inglés “Two Factor Authentication”.

Por lo expuesto anteriormente consideramos mandatorio diseñar un plan de ciberseguridad para ser implementado en CALSA (Cía. Argentina de Levaduras S.A.I.C), basándose en la Norma IEC 62443, que le permitirá alcanzar el nivel de madurez acorde al tipo de actividad e industria, adoptar estándares internacionales, incorporar la gestión de vulnerabilidades como una tarea periódica, generar nuevos procedimientos y políticas, educar a todos los empleados de la organización acerca de la importancia de la seguridad y entrenar a los principales actores, para lograr que la infraestructura del entorno industrial de CALSA (Cía. Argentina de Levaduras S.A.I.C), sea segura, defendiendo sus activos críticos de las amenazas internas y externas, reduciendo el tiempo y los costos asociados a los incidentes de ciberseguridad.

1.3. Marco Institucional

1.3.1. Historia

Desde sus orígenes CALSA (Cía. Argentina de Levaduras S.A.I.C) tuvo como objetivo ser líder y referente en materia de calidad y servicios para todo el mercado de la panificación. A través de los años la calidad de los productos y servicios marcaron el desarrollo de la panadería artesanal. Todo comenzó en 1923, con una marca que se hizo legendaria en la panadería argentina, Virgen, la marca de la levadura fresca que desde entonces se convirtió en la insignia de la compañía, siempre con la calidad y la innovación como una constante. En 1962 comenzó una ambiciosa etapa de expansión del negocio que implicó la ampliación del portfolio de productos, incorporando la línea de productos grasos. Como soporte a este ambicioso proyecto, en 1967 se fundó la Escuela de Panadería, que es hasta el día de hoy, un referente indiscutido del mercado. Durante la década del 70, incorporó en el mercado argentino los últimos avances tecnológicos para las panaderías, con el objetivo de impulsar el desarrollo del negocio de la panificación. En los años 80, se lanzó la línea de mejoradores para panes y la margarina Super, y en 1989 como resultado del proceso de investigación y desarrollo incorporó la margarina MTK. Durante la década del 90, se agrega al portfolio la Línea de Plata, una serie de premezclas que le permiten al panadero estandarizar su producción. El comienzo del siglo XXI posiciono a CALSA como la empresa líder de la panificación, consolidando como uno de sus principales los pilares la alta calidad en los productos y servicios, siendo líderes en innovación y desarrollo. En el 2001 decide trasladar la planta de levaduras de Hurlingham a la provincia de Tucumán, eso se debió a una decisión estratégica ya que el costo del flete para traer la melaza desde el norte era muy costo y la zona donde residía la planta estaba muy urbanizada y generaba trastornos logísticos y operativos. En ese proceso también se construye la planta de tratamiento de efluentes, en un claro compromiso con el medio ambiente. En el año 2004 CALSA paso a formar parte de un grupo global con sede en Inglaterra, fiel a sus orígenes, en donde la base es priorizar la tradición nacional del negocio panadero y artesanal (CALSA, Cia Argentina de Levaduras, s.f.).

Figura 15

Imágenes de cuadras de panaderías

Nota. Imagen extraída del sitio corporativo de CALSA (CALSA, Cia Argentina de Levaduras, s.f.).

1.3.2. Misión, Visión y Valores

Chiavenato (Chiavenato, 2007) define la misión organizacional como la declaración que expresa el propósito y el alcance de una empresa en términos de producto y mercado. Esta declaración define el rol de la organización de cara a la sociedad y representa su razón de ser y existir. Para definir la misión de la empresa CALSA (Cía. Argentina de Levaduras S.A.I.C), se plantearon y respondieron las siguientes preguntas: ¿Cuál es la razón de ser de la organización? ¿Qué papel desempeña la organización frente a la sociedad? ¿Cuál es la naturaleza del negocio? ¿Qué tipo de actividad realiza la organización?

La visión de una organización se refiere a las aspiraciones futuras de la empresa. Debe ser inspiradora y constituir el principal motivo por el cual todas las personas que forman parte de la organización dedican gran parte de su tiempo para alcanzar los objetivos establecidos.

A continuación, presentaremos la definición de la Misión, Visión y Valores de la empresa CALSA (Cía. Argentina de Levaduras S.A.I.C). En cuanto a la Misión, se ha establecido el objetivo de "Ser la empresa líder en el crecimiento, desarrollo y mejora de la experiencia de la panadería artesanal". Con relación a la Visión, se plantea "Ser el mejor..." con el fin de lograr un desempeño empresarial sostenible de clase mundial, enfocado en segmentos y experiencias artesanales dentro de nuestra región. Por último, los Valores de la empresa incluyen el profesionalismo, la comunicación abierta, la austeridad, la proactividad,

la cooperación y el compromiso. La definición de estos tres pilares ha permitido el desarrollo de objetivos estratégicos y su posterior comunicación a toda la organización.

1.4. Objetivos generales

El objetivo general de esta propuesta de intervención en el campo profesional es diseñar un plan de ciberseguridad basándose en la Norma IEC 62443, que le permita a la organización CALSA (Cía. Argentina de Levaduras S.A.I.C) adoptar una estrategia de ciberseguridad incorporando herramientas de gestión para preservar los activos críticos.

1.5. Objetivos particulares

Los objetivos particulares del trabajo final son:

- Relevar la situación actual de la red industrial de CALSA (Cía. Argentina de Levaduras S.A.I.C).
- Identificar los activos críticos.
- Análisis de la situación actual en relación con normas internacionales.
- Diagnosticar en base al relevamiento el nivel madurez, y los riesgos asociados.
- Identificar, mitigar las brechas y vulnerabilidades de seguridad actuales.
- Proponer un plan de mejoras que permitan incrementar el nivel de madurez del área industrial y la ciberseguridad.
- Diseñar un plan de ciberseguridad, que permitan asegurar los siguientes aspectos básicos: disponibilidad, integridad, confidencialidad y control de acceso.
- Crear programas de formación y capacitación para los colaboradores relacionados con la Industria 4.0.

Capítulo II

2.1 Acciones

2.1.1 Relevamiento

La metodología que se utilizó para obtener la información fue mediante el uso de cuestionarios de relevamiento y entrevistas con los responsables de la red industrial con el objetivo de esclarecer dudas que surgieron del proceso de obtención de la información. El resultado del análisis de la información obtenida permitirá identificar el estado actual, vulnerabilidades y riesgos de cada activo crítico involucrado en los procesos productivos y de control, como por ejemplo: obsolescencia, cantidad de equipos conectados a la red industrial, topología de la red, nivel de segmentación y aislamiento entre la red de IT, de sus siglas en inglés “Information Technologies” y la ICS, de sus siglas en inglés “Industrial Control Systems”, responsables, vulnerabilidades, riesgo, nivel de capacitación de los recursos humanos involucrados y planes futuros.

Las vulnerabilidades son debilidades en los sistemas o componentes, que se pueden presentar por problemas de diseño, falta de conocimiento en la configuración, y por la obsolescencia del equipamiento que cuando se adquirió las vulnerabilidades no estaban descubiertas pero que, con el paso del tiempo, los avances tecnológicos, las crecientes amenazas informáticas y la falta de actualización por parte de los fabricantes y las organizaciones quedan expuestas para que sea explotadas.

El riesgo es una probabilidad de que ocurra algún evento, que una amenaza explote una vulnerabilidad y tenga como consecuencia que se generen pérdidas para la organización con consecuencias directas, como reemplazar el activo dañado o consecuencias indirectas, como la reputación y/o permisos legales por violar las regulaciones existentes. La evaluación del riesgo debe evaluar el riesgo inicial, implementar acciones que contribuyan a mitigar el riesgo, y evaluar el riesgo residual. El proceso de gestión del riesgo tiene como principal función revisar la información recolectada, siendo el punto de partida para la toma de decisiones, por cada riesgo identificado hay 3 definiciones que se utilizan para su clasificación y que se explican en la siguiente Tabla (IEC/TS 62443, 2009).

Tabla 5

Clasificación de los Riesgos

Clasificación	Definición
Intolerable	Se deberá reemplazar o abandonar el sistema en riesgo, en caso de no ser posible la vulnerabilidad debe ser controlada y limitar la exposición
Tolerable	Los riesgos son reducidos de forma aceptable.
Aceptable	La reducción del riesgo no es necesaria y puede proceder sin intervención.

Nota. Extraída de The Cyber Security Body of Knowledge (The Cyber Security Body of Knowledge, 2019).

El propósito de la evaluación y gestión de riesgos es comunicar los resultados y asegurarse que las decisiones que se tomen sean ejecutadas de forma exitosa para minimizar los riesgos, teniendo un equilibrio razonable entre riesgos aceptables y mitigados.

Los cuestionarios de relevamiento están orientados a identificar todos los activos que son parte del proceso productivo, su nivel de riesgo, el tipo de comunicación, la forma de conexión, y acceso remoto, entre ellos podemos citar a los instrumentos de control, PLC de sus siglas en inglés “Programmable Logic Controller”, switchs, servidores y clientes delgados.

2.1.2 Identificación de activos

La norma IEC 62443 considera que la base para diseñar un plan de ciberseguridad es poseer un inventario de los activos. Los activos están clasificados como físicos, lógicos y humanos. Por activo físico se considera a cualquier componente o grupo de componentes físicos, aquí podemos incluir a los sistemas de control, redes, salas de operaciones, cualquier objeto físico que participe en el proceso productivo. Los activos lógicos son la propiedad intelectual, patentes, conocimientos del proceso, reputación o cualquier otra información que sea considerada confidencial y que su perdida afecte directamente a la organización dejando de tener una ventaja competitiva respecto a la competencia o genere una mala reputación de la organización. Sobre los activos humanos debemos mencionar que son las personas, sus conocimientos y habilidades asociadas al proceso productivo. Los activos pueden valorarse de forma cuantitativa o cualitativa. La valoración cuantitativa, es cuando la pérdida del activo está directamente ligada a la pérdida económica, por el costo de reemplazar el activo, perdida en ventas, u otras formas de expresar estas pérdidas. Cuando se refiere a la valoración cualitativa la forma de expresarla es más abstracta, como alto, bajo o medio impacto, luego esta valoración

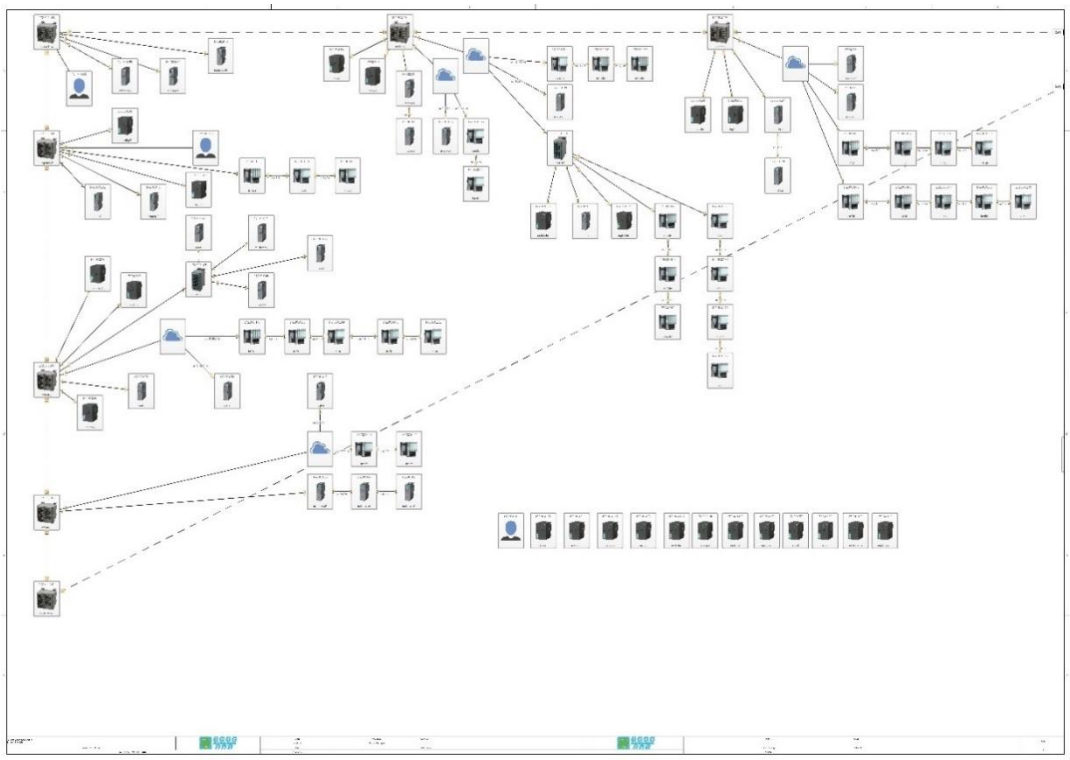
debe justificarse con un análisis cuantitativo que termine valorizando ese riesgo (IEC/TS 62443, 2009).

2.1.3 Topología

En la Figura 17 y la Figura 18 podemos apreciar la topología actual de la red industrial de CALSA en su Planta de Lanús, para obtenerla se utilizó el software "PROFINET Topology Software PROscan", el escaneo final es exportado en PDF y se agregó en los Anexos de este documento. Se puede observar cómo los activos involucrados en el proceso se conectan físicamente a través de un anillo de fibra óptica y los switchs marca Siemens de la familia Scalance X (Siemens, SCALANCE, s.f.), dentro de la topología se identifican los sectores de Caldera, Balanza Planta 2, Desodo, Margarina, Fraccionamiento, Sala de Servidores, Tanques e Hidrogenación.

Figura 16

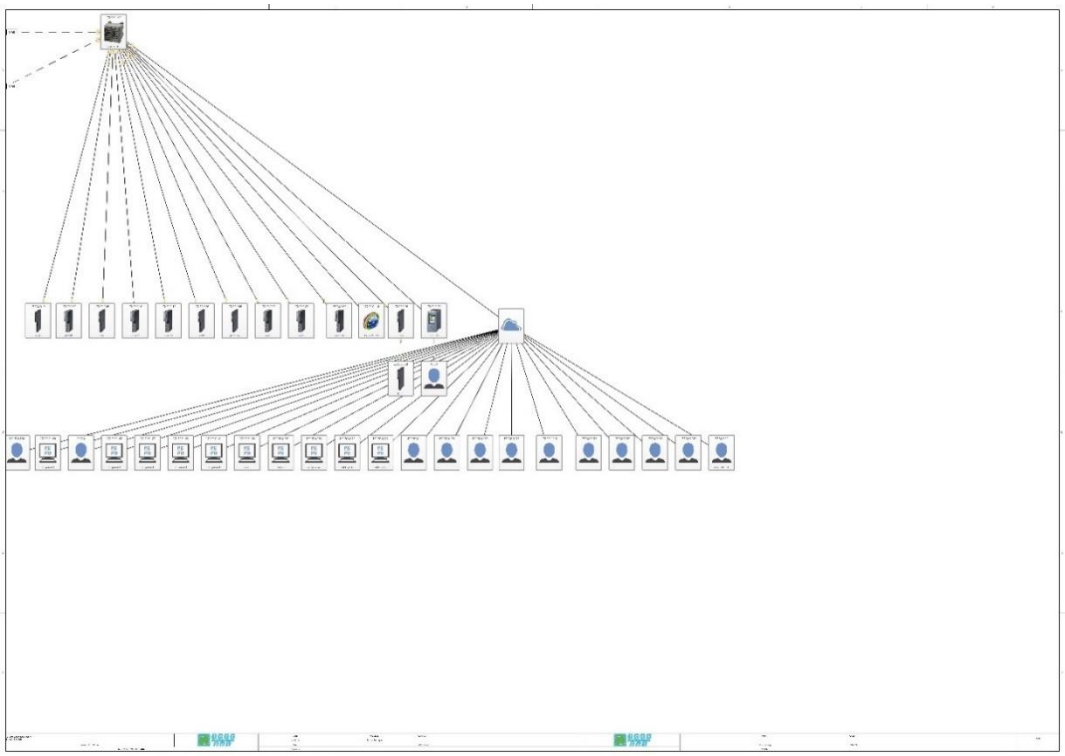
Topología de la red industrial de CALSA, Planta Lanús, Parte 1



Nota. Figura generada a través de PROFINET Topology Software PROscan

Figura 17

Topología de la red industrial de CALSA, Planta Lanús, Parte 2



Nota. Figura generada a través de PROFINET Topology Software PROscan

2.1.4 Instrumentos de Control

Los instrumentos de control están situados en la red de campo de una red industrial, están en el nivel 0 de la Figura 2, en este nivel podemos encontrar sensores, caudalímetros, actuadores, entre otros. Estos dispositivos transmiten información de los procesos en tiempo real. La Tabla 6 identifica a los activos, criticidad y riesgo según su clasificación.

Tabla 6

Instrumentos, Clasificación del Tipo de Activo, Criticidad y Riesgo

Sector	Tipo de Equipo	Activo	Criticidad	Riegos
			Clasificación	
Planta Lanús	Instrumentos red ASI	Físico	Baja	Aceptable
Planta Lanús	Instrumentos red Profi PA DP	Físico	Baja	Aceptable
Planta Lanús	Caudalímetros	Físico	Baja	Aceptable
Planta Lanús	Variadores/Arrancadores Suaves	Físico	Baja	Aceptable
Mantenimiento	Pliscon/Programación Vega	Físico	Baja	Aceptable

Nota. De producción propia en base al relevamiento realizado.

La información que nos muestra la Tabla 8, es que los dispositivos de campo no utilizan la norma 802.11 creada por el IEEE, de sus siglas en ingles “Institute of Electrical and Electronics Engineers”, sino utilizan una red Wireless dedicada y propietaria para los caudalímetros y variadores.

Tabla 7

Tipos de Instrumentos y su Comunicación con la red Industrial

Sector	Tipo de Equipo	Bluetooth	Wireless	Wi Fi
			Comunicación	
Planta Lanús	Instrumentos red ASI	No	No	No
Planta Lanús	Instrumentos red Profi PA DP	No	No	No
Planta Lanús	Caudalímetros	No	Si	No
Planta Lanús	Variadores/Arrancadores Suaves	No	Si	No
Mantenimiento	Pliscon/Programación Vega	Si	No	No

Nota. De producción propia en base al relevamiento realizado.

La Tabla 9 nos permite identificar contra qué tipo de activos se conectan los instrumentos de campo, en el entorno industrial (ICS) de sus siglas en inglés “Industrial Control Systems”, los instrumentos se conectan con el PLC Central, PLC aislado y los switchs de la red IT y OT.

Tabla 8

Tipos de Instrumentos y su Interconexión con PLC y Switchs

Sector	Tipo de Equipo	PLC Central	PLC Aislado	Switch IT	Switch OT
			Interconexión		
Planta Lanús	Instrumentos red ASI	Si	No	No	No
Planta Lanús	Instrumentos red Profi PA DP	Si	No	No	No
Planta Lanús	Caudalímetros	No	No	Si	No
Planta Lanús	Variadores/Arrancadores Suaves	Si	Si	No	No
Mantenimiento	Pliscon/Programación Vega	No	No	No	No

Nota. De producción propia en base al relevamiento realizado.

En la Tabla 10 nos muestra información sobre los tipos de puertos que tienen disponibles para conectarse a los instrumentos, entre ellos están los puertos USB de sus siglas en inglés “Universal Serial Bus”, ethernet y 4-20.

Tabla 9

Instrumentos de Campos y Puertos habilitados

Sector	Tipo de Equipo	USB	Ethernet	C4-20
			Tipo de Puertos	
Planta Lanús	Instrumentos red ASI	Si	No	No
Planta Lanús	Instrumentos red Profi PA DP	Si	No	No
Planta Lanús	Caudalímetros	No	No	Si
Planta Lanús	Variadores/Arrancadores Suaves	Si	Si	No
Mantenimiento	Pliscon/Programación Vega	No	No	No

Nota. De producción propia en base al relevamiento realizado.

Las formas de acceso remoto indicadas en la Tabla 11 nos permite conocer a cuantos proveedores se les otorga acceso y de que tipo, mediante qué sistema de conexión, y si adoptan MFA, de sus siglas en ingles “Multi Factor Authentication” para completar el proceso de autenticación.

Tabla 10

Formas de Acceso Remoto a los Instrumentos de Campo

Sector	Tipo de Equipo	USB	Asistencia	Conexión	MFA
			Acceso Remoto		
Planta Lanús	Instrumentos red ASI	0	Autex	VPN Client	No
Planta Lanús	Instrumentos red Profi PA DP	0	Autex	VPN Client	No
Planta Lanús	Caudalímetros	2	NA	Si	NA
Planta Lanús	Variadores/Arrancadores Suaves	0	NA	No	NA
Mantenimiento	Pliscon/Programación Vega	0	NA	No	NA

Nota. De producción propia en base al relevamiento realizado.

2.1.5 Terminales

Las terminales son utilizadas por los operadores de los procesos productivos para conectarse de forma remota mediante el uso del protocolo RDP, de sus siglas en ingles “Remote Desktop Protocol” y gestionar las distintas plantas de la red industrial (ICS) de sus siglas en inglés “Industrial Control Systems”, aquí podemos observar que hay Thin Clients, notebooks, desktops y paneles de control. Estos dispositivos transmiten información de los procesos en tiempo real. En la Tabla 12 se observa el tipo de equipo, clasificación del activo, criticidad y riesgo según su clasificación.

Tabla 11

Terminales, Clasificación del Tipo de Activo, Criticidad y Riesgo

Sector	Tipo de Equipo	Activo	Criticidad	Riegos
			Clasificación	
Desodo	Thin Client	Físico	Media	Tolerable
PNB	Thin Client	Físico	Media	Tolerable
Blanqueo	Thin Client	Físico	Media	Tolerable
Hidrogenación	Thin Client	Físico	Media	Tolerable
Interesterificación	Thin Client	Físico	Media	Tolerable
Fraccionamiento	Thin Client	Físico	Media	Tolerable
Margarina 1-2	Thin Client	Físico	Media	Tolerable
Margarina 3	Thin Client	Físico	Media	Tolerable
Shortening	Thin Client	Físico	Media	Tolerable
Calderas	Thin Client	Físico	Media	Tolerable
RM	Thin Client	Físico	Media	Tolerable
Balanza Pt2	Thin Client	Físico	Media	Tolerable
Balanza Pt4	Desktop	Físico	Media	Tolerable
BI	Desktop Profinet	Físico	Media	Tolerable
Calidad	Thin Client	Físico	Media	Tolerable
Túnel	Desktop	Físico	Media	Tolerable
Salida del túnel	Desktop	Físico	Media	Tolerable
Mantenimiento	Notebook	Físico	Media	Tolerable
Mantenimiento	Panel	Físico	Media	Tolerable
Margarina	Panel	Físico	Media	Tolerable
Shortening	Panel	Físico	Media	Tolerable
Robot	Panel	Físico	Media	Tolerable
Paletizadora	Panel	Físico	Media	Tolerable
Salida del túnel	Desktop	Físico	Media	Tolerable
Planta Lanús	Específicos	Físico	Media	Tolerable
ETP	Panel	Físico	Media	Tolerable

Nota. De producción propia en base al relevamiento realizado.

La Tabla 13 nos muestra como es la forma de comunicación dentro de la red industrial (ICS) de sus siglas en inglés “Industrial Control Systems”, de los distintos tipos de terminales que permiten la operación de los procesos productivos y contra que otros equipos se comunican.

Tabla 12

Tipos de Terminales y Tecnologías de Comunicación

Sector	Tipo de Equipo	Bluetooth	Wireless	Wi Fi
			Comunicación	
Desodo	Thin Client	No	No	No
PNB	Thin Client	No	No	No
Blanqueo	Thin Client	No	No	No
Hidrogenación	Thin Client	No	No	No
Interesterificación	Thin Client	No	No	No
Fraccionamiento	Thin Client	No	No	No
Margarina 1-2	Thin Client	No	No	No
Margarina 3	Thin Client	No	No	No
Shortening	Thin Client	No	No	No
Calderas	Thin Client	No	No	No
RM	Thin Client	No	No	No
Balanza Pt2	Thin Client	No	No	No
Balanza Pt4	Desktop	Si	No	No
BI	Desktop Profinet	Si	No	Si
Calidad	Thin Client	No	No	No
Túnel	Desktop	No	No	Si
Salida del túnel	Desktop	No	No	Si
Mantenimiento	Notebook	Si	No	Si
Mantenimiento	Panel	No	No	No
Margarina	Panel	No	No	No
Shortening	Panel	Si	No	No
Robot	Panel	Si	No	No
Paletizadora	Panel	Si	No	No
Salida del túnel	Desktop	No	No	No
Planta Lanús	Específicos	No	No	No
ETP	Panel	No	No	No

Nota. De producción propia en base al relevamiento realizado.

La Tabla 14 ilustra la manera en que los dispositivos se interconectan dentro de la red industrial (ICS), de sus siglas en inglés "Industrial Control Systems". Muestra los diferentes tipos de terminales que permiten el funcionamiento de los procesos productivos y con qué otros equipos se conectan.

Tabla 13

Tipos de Terminales y su Conexión contra los PLC y Switchs

Sector	Tipo de Equipo	PLC Central	PLC Aislado	Switch IT	Switch OT
			Interconexión		
Desodo	Thin Client	No	No	Si	No
PNB	Thin Client	No	No	Si	No
Blanqueo	Thin Client	No	No	Si	No
Hidrogenación	Thin Client	No	No	Si	No
Interesterificación	Thin Client	No	No	Si	No
Fraccionamiento	Thin Client	No	No	Si	No
Margarina 1-2	Thin Client	No	No	Si	No
Margarina 3	Thin Client	No	No	Si	No
Shortening	Thin Client	No	No	Si	No
Calderas	Thin Client	No	No	Si	No
RM	Thin Client	No	No	Si	No
Balanza Pt2	Thin Client	No	No	Si	No
Balanza Pt4	Desktop	No	No	Si	No
BI	Desktop Profinet	Si	No	No	No
Calidad	Thin Client	Si	No	Si	No
Túnel	Desktop	No	Si	No	No
Salida del túnel	Desktop	No	Si	Si	No
Mantenimiento	Notebook	No	Si	Si	No
Mantenimiento	Panel	No	Si	No	No
Margarina	Panel	No	Si	No	No
Shortening	Panel	No	Si	No	No
Robot	Panel	No	Si	No	No
Paletizadora	Panel	No	Si	No	No
Salida del túnel	Desktop	No	Si	No	No
Planta Lanús	Específicos	No	Si	No	No
ETP	Panel	No	Si	No	No

Nota. De producción propia en base al relevamiento realizado.

La Tabla 15 nos permite visualizar los tipos de puertos que son compatibles con las terminales utilizadas en la red industrial (ICS), de sus siglas en inglés "Industrial Control Systems". Los puertos predominantes son el USB y el Ethernet

Tabla 14

Tipos de Terminales y los puestos Soportados

Sector	Tipo de Equipo	USB	Ethernet	Tarjeta	C4-20
			Tipos de Puertos		
Desodo	Thin Client	Si	Si	No	No
PNB	Thin Client	Si	Si	No	No
Blanqueo	Thin Client	Si	Si	No	No
Hidrogenación	Thin Client	Si	Si	No	No
Interesterificación	Thin Client	Si	Si	No	No
Fraccionamiento	Thin Client	Si	Si	No	No
Margarina 1-2	Thin Client	Si	Si	No	No
Margarina 3	Thin Client	Si	Si	No	No
Shortening	Thin Client	Si	Si	No	No
Calderas	Thin Client	Si	Si	No	No
RM	Thin Client	Si	Si	No	No
Balanza Pt2	Thin Client	Si	Si	No	No
Balanza Pt4	Desktop	Si	Si	Si	No
BI	Desktop Profinet	Si	Si	Si	No
Calidad	Thin Client	Si	Si	No	No
Túnel	Desktop	Si	Si	Si	No
Salida del túnel	Desktop	Si	Si	Si	No
Mantenimiento	Notebook	Si	Si	Si	No
Mantenimiento	Panel	Si	Si	No	No
Margarina	Panel	Si	Si	No	No
Shortening	Panel	Si	Si	Si	No
Robot	Panel	Si	Si	Si	No
Paletizadora	Panel	Si	Si	Si	No
Salida del túnel	Desktop	No	Si	No	No
Planta Lanús	Específicos	No	No	No	No
ETP	Panel	No	No	No	No

Nota. De producción propia en base al relevamiento realizado.

La información que presenta la Tabla 16 es relevante acerca de los tipos de terminales y los métodos utilizados por los proveedores para acceder de forma remota a la red industrial (ICS), de sus siglas en inglés "Industrial Control Systems", con el propósito de brindar soporte. Esta tabla detalla los métodos de conexión utilizados, el tipo de acceso remoto, así como las medidas de seguridad adicionales implementadas para garantizar la protección de la red. La inclusión de esta información resulta de gran importancia, ya que permite comprender cómo los proveedores se conectan de manera remota a los sistemas de control industrial y los restricciones de seguridad adoptadas para las conexiones.

Tabla 15

Tipos de Terminales y forma de Acceso Remoto

Sector	Tipo de Equipo	USB	Asistencia	VPN	MFA
			Acceso Remoto		
Desodo	Thin Client	No	NA	NA	NA
PNB	Thin Client	No	NA	NA	NA
Blanqueo	Thin Client	No	NA	NA	NA
Hidrogenación	Thin Client	No	NA	NA	NA
Interesterificación	Thin Client	No	NA	NA	NA
Fraccionamiento	Thin Client	No	NA	NA	NA
Margarina 1-2	Thin Client	No	NA	NA	NA
Margarina 3	Thin Client	No	NA	NA	NA
Shortening	Thin Client	No	NA	NA	NA
Calderas	Thin Client	No	NA	NA	NA
RM	Thin Client	No	NA	NA	NA
Balanza Pt2	Thin Client	No	NA	NA	NA
Balanza Pt4	Desktop	Si	IT	Client	No
BI	Desktop Profinet	Si	Autex/Buhler	Si	No
Calidad	Thin Client	No	NA	NA	NA
Túnel	Desktop	Si	NA	NA	NA
Salida del túnel	Desktop	Si	Trend	Client	No
Mantenimiento	Notebook	Si	NA	NA	NA
Mantenimiento	Panel	Si	NA	NA	NA
Margarina	Panel	Si	NA	NA	NA
Shortening	Panel	Si	NA	NA	NA
Robot	Panel	Si	NA	NA	NA
Paletizadora	Panel	Si	NA	NA	NA
Salida del túnel	Desktop	Si	NA	NA	NA
Planta Lanús	Específicos	Si	NA	NA	NA
ETP	Panel	Si	NA	NA	NA

Nota. De producción propia en base al relevamiento realizado.

2.1.6 PLC

La pirámide de automatización industrial sitúa a los PLC, de sus siglas en inglés “Programmable Logic Controllers” como parte de la red de control. Los PLC se encargan de establecer la comunicación entre la red de campo y la red de supervisión.

Sobre los PLC y las Tecnologías de Comunicación utilizados por CALSA podemos mencionar, ubicación, función, como están clasificados de estos activos, nivel de criticidad y el riesgo asociado a cada uno de ellos:

- Sector: Sala de Servidores
- Tipo de Equipo: PLC Central

- Activo: Físico
- Criticidad; Muy Alta
- Riesgo: Tolerable

Respecto a cómo el PLC Central se interconectan con los distintos equipos dentro del entorno industrial podemos afirmar que no utiliza USB, Bluetooth, ni ningún tipo de tecnología inalámbrica, lo hace vía Ethernet.

2.1.7 Networking

En esta sección obtendremos la información del equipamiento de Networking que conecta a todos los dispositivos en el entorno industrial (ICS) de sus siglas en inglés "Industrial Control Systems", en la Tabla 16, podemos identificar el tipo de activo, criticidad y riesgo según su clasificación.

Tabla 16

Networking, medios Utilizados para la Comunicación

Sector	Soporta VLAN	Activo	Criticidad	Riesgo
			Clasificación	
Sala Servidores	No	Físico	Muy Alta	Tolerable
Sala de Operaciones IT	Si	Físico	Muy Alta	Tolerable
Sala de Operaciones OT	No	Físico	Muy Alta	Tolerable
Tableros de Distribución	No	Físico	Media	Tolerable

Nota. De producción propia en base al relevamiento realizado.

La Tabla 17, nos indica contra qué tipo de activos dentro de la infraestructura de la red industrial (ICS) de sus siglas en inglés "Industrial Control Systems" se conectan los dispositivos de Networking.

Tabla 17

Netwoking, medios Utilizados para el Conexionado

Sector	Bluetooth	Wireless	Fibra Óptica	Wi Fi
		Comunicación		
Sala Servidores	No	No	Si	No
Sala de Operaciones IT	No	No	No	No
Sala de Operaciones OT	No	No	Si	No
Tableros de Distribución	No	No	No	No

Nota. De producción propia en base al relevamiento realizado.

De la Tabla 18, obtenemos la información de cuál es la forma de conectarse físicamente a los equipos de networking en la infraestructura de la red industrial.

Tabla 18

Netwoking, tipo de Puertos Soportados

Sector	USB	Ethernet	C4-20
	Tipos de Puerto		
Sala Servidores	No	Si	No
Sala de Operaciones IT	No	Si	No
Sala de Operaciones OT	No	Si	No
Tableros de Distribución	No	Si	No

Nota. De producción propia en base al relevamiento realizado.

La Tabla 19, nos indica de qué manera los proveedores que hacen soporte en la infraestructura de la red industrial (ICS) de sus siglas en inglés “Industrial Control Systems”, se conectan a los activos de networking para dar soporte remoto.

Tabla 19

Networking y las formas de acceso remoto

Sector	USB	Asistencia	VPN	MFA
	Acceso Remoto			
Sala Servidores	Si	Autex	Client	No
Sala de Operaciones IT	No	IT	Client	Si
Sala de Operaciones OT	Si	Autex	Client	No
Tableros de Distribución	Si	Autex	Client	No

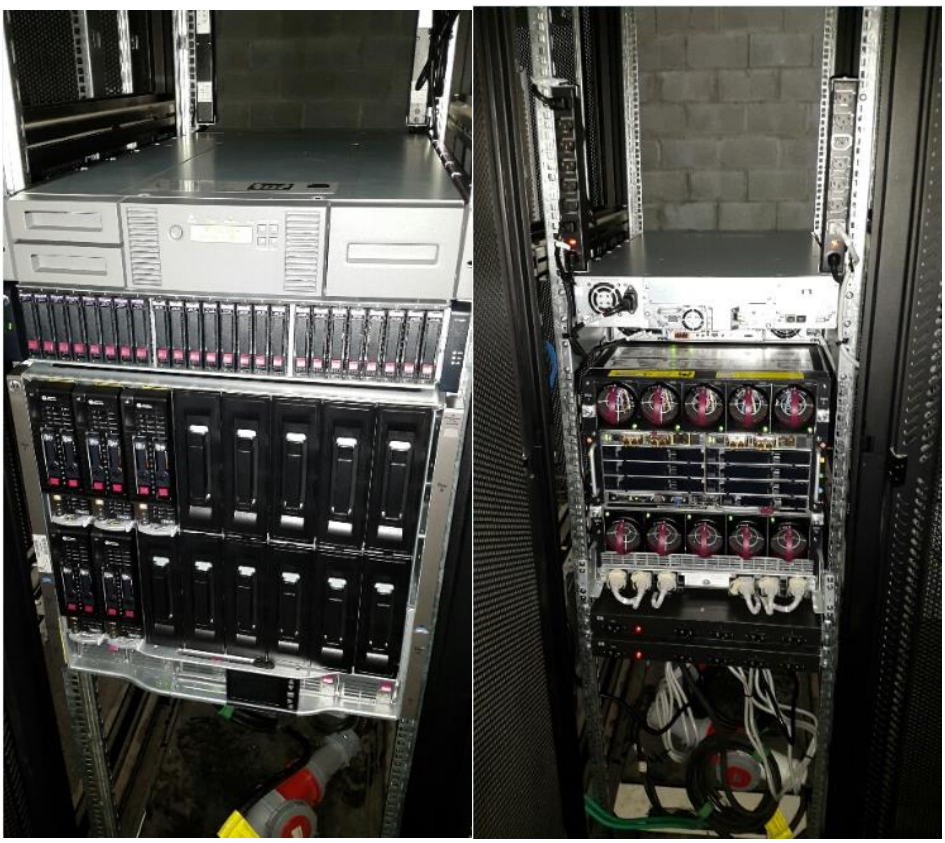
Nota. De producción propia en base al relevamiento realizado.

2.1.8 Servidores

La función primordial de los servidores consiste en la ejecución de aplicaciones que respaldan los procesos productivos en el ámbito industrial. En este sentido, en el entorno de CALSA, se ha implementado un chasis de HP Blade System C7000, desarrollado por Hewlett-Packard, el cual está compuesto por cinco servidores físicos HP Proliant, dos switches SAN Brocade, dos dispositivos de almacenamiento HP P2000 y una unidad de Backup con capacidad para 24 unidades, conocida como Library MSL 2024. La Figura 19 proporciona una representación visual del estado y la disposición de dicho equipamiento en dos racks de 42 unidades cada uno, ubicados en la sala de servidores de Planta 6 de CALSA.

Figura 18

Blade System, Servidores, Unidad de Backup y Storage HP.

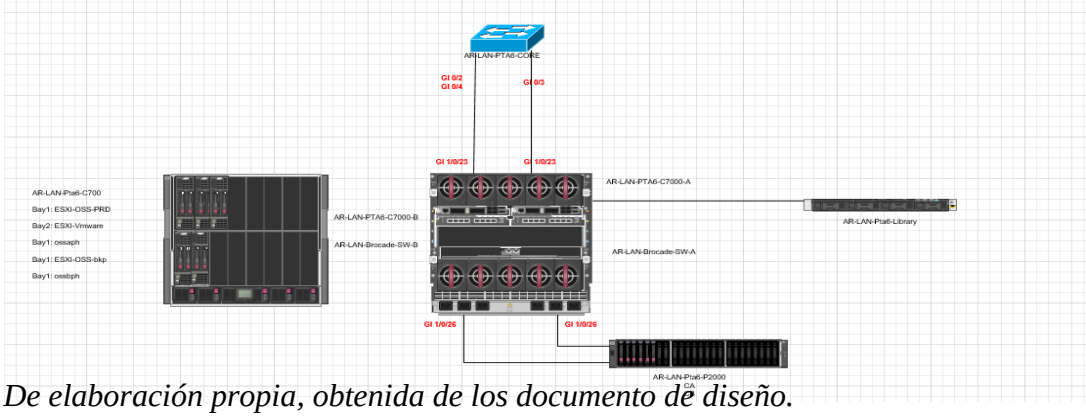


Nota. Fotos obtenidas del relevamiento realizado.

La configuración del conjunto de servidores se describe de la siguiente manera: el chasis HP Blade System C7000 alberga a cinco servidores físicos HP Proliant. Mediante los dos switches de fibra óptica SAN Brocade, se publican las LUN, de sus siglas en inglés “Logical Unit Number” provenientes de los dos almacenamientos HP P2000, además se conecta la unidad de respaldo HP Library MSL 2024. Tres de los cinco servidores tienen instalada la plataforma de virtualización Vmware, específicamente la versión ESXI 5.5, que al momento de la implementación fue la versión aprobada y compatible con los sistemas de Siemens. En los dos servidores físicos restantes, se ha implementado una configuración redundante del sistema "Historian". La Figura 20 representa la arquitectura detallada mencionada.

Figura 19

Documentación de Diseño de la Infraestructura HP

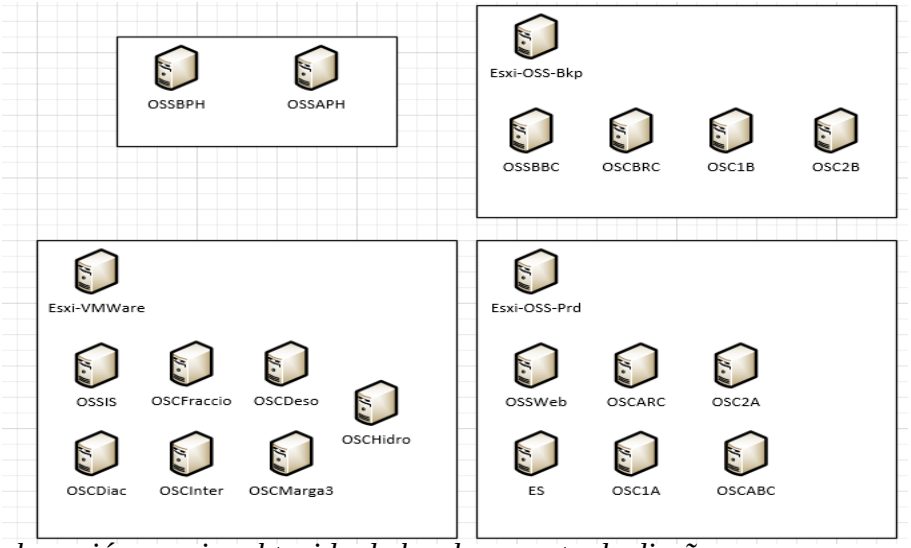


Nota. De elaboración propia, obtenida de los documento de diseño.

La distribución de los servidores virtualizados dentro de la infraestructura de Vmware se muestra en la Figura 21. El servidor denominado ESXI-Vmware se encarga de alojar las máquinas virtuales correspondientes a las plantas productivas, las cuales son accedidas utilizando el protocolo RDP, de sus siglas en ingles "Remote Desktop Protocol" por los operadores de los procesos productivos. Por su parte, en el servidor ESXI-OSS-PRD se encuentran instaladas las máquinas virtuales que respaldan los siguientes procesos: Ingeniería, Servidor Principal Producción 1, Servidor Principal Producción 2, Servidor Principal Batch y Servidor Principal Route Control. El servidor ESXI-OSS-BKP brinda redundancia al servidor ESXI-OSS-PRD, asegurando la continuidad operativa. Por último, los servidores OSSAPH y OSSBPH son los servidores físicos en los cuales se ejecutan el sistema Principal Process Historian ambos servidores utilizan un sistema de redundancia propietario de Siemens.

Figura 20

Distribución de los servidores ESXI y Process Historian

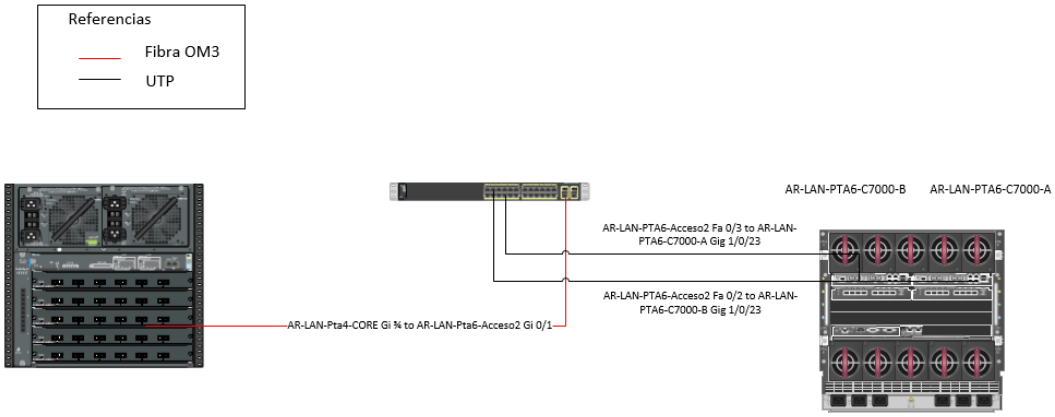


Nota. De elaboración propia, obtenida de los documento de diseño.

La Figura 22 ilustra la conexión del anillo de fibra óptica utilizado para la red industrial con el Switch Cisco Systems de la red de IT, de sus siglas en inglés “Information Technologies”, ubicado en la sala de servidores de la Planta 6 de CALSA. Esta interconexión permite establecer la comunicación entre la red industrial y la red de IT, posibilitando el intercambio de datos y la integración de los sistemas industriales y empresariales.

Figura 21

Topología de Conexión de los Servidores OT



Nota. De producción propia basada en el relevamiento realizado.

La Tabla 20 muestra los diferentes tipos de tecnologías utilizadas para la comunicación en la red industrial. Estas tecnologías incluyen Bluetooth, Wi-Fi, fibra óptica y redes inalámbricas. Cada una de estas tecnologías desempeña un papel crucial en la infraestructura de comunicaciones, facilitando la transferencia eficiente y confiable de datos en el entorno industrial.

Tabla 20

Servidores y la Tecnología de Conexión

Sector	Equipo	Bluetooth	Wireless	Fibra Óptica	Wi Fi
			Comunicación		
Planta Lanús	Gateway	No	Si	No	No
Sala de Servidores	Servidor PC	No	No	Si	No
PLC Central	PLC S7	No	No	Si	No
Sala de Servidores	Servidor Buhler	No	No	Si	No

Nota. De producción propia en base al relevamiento realizado.

La Tabla 21 representa a los activos de la red industrial que están involucrados en las comunicaciones entre los distintos niveles de la red, nos ayuda a comprender cómo interactúan y se comunican entre sí los diversos elementos que componen la red industrial.

Tabla 21

Los Servidores y su Comunicación contra otros Activos

Sector	Equipo	PLC Central	PLC Aislado	Switch IT	Switch OT
			Interconexión		
Planta Lanús	Gateway	Si	No	No	Si
Sala de Servidores	Servidor PC	Si	No	No	Si
PLC Central	PLC S7	Si	No	No	Si
Sala de Servidores	Servidor Buhler	Si	No	No	Si

Nota. De producción propia en base al relevamiento realizado.

En la Tabla 22 nos permite visualizar que tipos de puertos soportan los servidores activos en una red industrial, utilizados para lograr de manera eficiente y confiable la conectividad y comunicación con otros dispositivos y sistemas. Algunos ejemplos de puertos comunes que podrían estar presentes en servidores industriales son: ethernet, USB, serie o RS-232, fibra óptica y C4-20. Es importante tener en cuenta que la disponibilidad y el tipo de puertos pueden variar según el modelo y las especificaciones de los servidores utilizados en la red industrial en particular.

Tabla 22

Los Servidores y los Tipos de Puertos que Soportan

Sector	Equipo	USB	Ethernet	C4-20
			Tipos de Puertos	
Planta Lanús	Gateway	No	Si	No
Sala de Servidores	Servidor PC	No	Si	No
PLC Central	PLC S7	No	Si	No
Sala de Servidores	Servidor Buhler	No	Si	No

Nota. De producción propia en base al relevamiento realizado.

En la Tabla 23 se describe en detalle como los proveedores pueden utilizar diferentes métodos para conectarse a una red industrial, y las medidas de seguridad adicionales adoptadas pueden variar según los requisitos de cada organización. Las medidas de seguridad adicionales

pueden variar según la industria, el tamaño de la organización y los requisitos de seguridad específicos.

Tabla 23

Los Servidores y las formas de Acceso Remoto

Sector	Equipo	USB	Asistencia	VPN	MFA
			Acceso Remoto		
Planta Lanús	Gateway	Si	Autex	Client	No
Sala de Servidores	Servidor PC	Si	Autex	Client	No
PLC Central	PLC S7	Si	Autex	Client	No
Sala de Servidores	Servidor Buhler	Si	Autex	Client	No

Nota. De producción propia en base al relevamiento realizado.

2.1.9 Análisis

En esta sección se realizará el análisis en base a la información obtenida del relevamiento. Aquí identificamos a los equipos e instalaciones que tienen criticidad muy alta para la organización, que son vitales para la continuidad del negocio y los procesos productivos. La Tabla 24 nos permite identificar el listado de activos críticos que están alojados en la “Sala de Servidores de Planta 6”, lugar en donde se encuentra instalado el PLC Central, la fibra óptica que interconecta a todos los PLC, los servidores HP, la unidad de Backup y los switches de red, dicha Sala de Servidores es un componente clave de la infraestructura, allí dentro están los activos más importantes para el funcionamiento de la red industrial. El PLC Central es responsable de la automatización y control de los procesos productivos, mientras que los servidores HP proporcionan soporte para las aplicaciones industriales. La identificación de estos equipos e instalaciones como críticos y vitales resalta su importancia para la continuidad del negocio. Su correcto funcionamiento y disponibilidad son fundamentales para garantizar la operatividad y eficiencia de los procesos productivos en la organización. Cabe mencionar que dichos servidores no cuentan con contrato de garantía vigentes y están discontinuados por el fabricante.

Tabla 24

Listado de los Activos Críticos

Sector	Equipo	Activo	Criticidad	Riesgo
			Clasificación	
Sala de Servidores	PLC Central	Físico	Muy Alta	Tolerable
Sala de Servidores	Fibra Óptica	Físico	Muy Alta	Tolerable
Sala de Operaciones IT	Fibra Óptica	Físico	Muy Alta	Tolerable
Planta Lanús	Gateway	Físico	Muy Alta	Tolerable
Sala de Servidores	Servidor PC	Físico	Muy Alta	Tolerable
Sala de Servidores	PLC S7	Físico	Muy Alta	Tolerable
Sala de Servidores	Servidor Buhler	Físico	Muy Alta	Tolerable
Sala de Servidores	Blade HP	Físico	Muy Alta	Tolerable

Nota. De producción propia en base al relevamiento realizado.

En la Tabla 25 tenemos la definición de los tipos de actores considerados, aquí podemos observar que puede haber amenazas internas y externas. Como amenaza interna se consideran a los empleados dentro de la organización que por desconocimiento y/o mala intención generen un tipo de brecha de seguridad. En la categoría de amenazas externas la amplitud es mayor ya que puede podemos encontrar desde “buscadores de aventuras” hasta grupos de activismo impulsados por los siguientes motivos: causar daños e interrumpir servicios críticos, políticos e ideológicos, obtención de beneficios económicos robando datos personales y financieros que son utilizados para realizar fraudes y por ultimo venganza o represalias a organizaciones o instituciones que las consideran responsables de alguna situación que afecta a la sociedad. Debemos destacar que los grupos de ciberterrorismo son entidades criminales y sus acciones son ilegales, los ataques que realizan estos grupos pueden tener consecuencias graves para la seguridad, la economía y la estabilidad de un país o una organización. Es muy importante contar con medidas de ciberseguridad robustas y promover la cooperación internacional para combatir estas amenazas.

Tabla 25

Actores de Amenazadas (Threat Actor)

Actor	Nivel del actor de la amenaza
No dirigido	Actor interno con causa de daño intencional o no, como virus.
Buscador de Emociones	Actor externo con medios muy limitados, con la intención de causar daño, pero sin ser dirigido a un sector industrial específico.
Ciber Delincuente	Actor externo (individuo u organización) con medios limitados, pero con determinación a un sector industrial específico (por ejemplo, empleado despedido).
Grupo Terrorista	Organización con recursos (p. ej., terrorismo, prácticas comerciales desleales) y con cierta determinación para un sector industrial específico.
Grupos Hacktivistas	Organización con medios ilimitados y una determinación muy fuerte para una organización, empresa o instalación de fabricación específica.

Nota. Extraído del Cuestionario de Estratificación del Riesgo.

A continuación, en la Tabla 26 se explican los distintos niveles de amenazas que varían en su grado de peligrosidad. Estos niveles incluyen: bajo, moderado, sustancial, severo y crítico. Estos niveles son utilizados para evaluar y comunicar en grado de riesgo asociado a las amenazas identificadas.

Tabla 26

Niveles de Amenazas (Threat Levels)

Escala	Nivel de Amenaza
Bajo	Ataque muy poco probable, impacto limitado y fácilmente gestionadas
Moderado	Ataque posible pero no probable, requiere medidas de seguridad y respuestas adecuadas para mitigar el impacto
Sustancial	Es probable un ataque, riesgo significativo y serios impactos, medidas de seguridad más rigurosas
Severo	Es muy probable, riesgo muy alto e impacto grave
Crítico	Es muy probable que se produzca el ataque en el corto plazo, daños significativos, interrupciones masivas y pérdida de vidas.

Nota. Extraído del Cuestionario de Estratificación del Riesgo.

El resultado del cuestionario de estratificación de riesgo nos permite observar que los actores de los ataques son los usuarios internos, mientras que los tipos de amenazas y la probabilidad de ocurrencia es moderada, obteniendo un riesgo de impacto y daño moderado, se requerirán medidas de ciber seguridad adicionales y una respuesta adecuada para evitar o minimizar el impacto.

Tabla 27

Planta Lanús, Cuestionario de Estratificación del Riesgo

Categoría	Criterio	Aplicabilidad al sitio/fábrica
Actor de Amenaza	Nivel del Actor de Amenaza	Actor de amenazas interno con causa de daño unitario, como virus, robots, etc.
Nivel de Amenaza	Nivel de Amenaza	Ataque es posible pero no probable
Conectividad	Niveles de Conectividad	La red ICS está conectada a la red LAN Corporativa
Acceso de Usuarios	Nivel de accesos	Los niveles de acceso segregan funciones, pero no identifican a los usuario individuales ni control de acceso privilegiado.
Gobierno	Roles y Responsabilidades	No hay definida una cadena de responsabilidad para la ciberseguridad de ICS
	Inventario Industrial	Se relevan y gestionan inventarios físicos, lógicos y de aplicaciones. Los inventarios se revisan periódicamente y como mínimo cada vez que se modifica la red ICS
	Revisiones de Ciber Seguridad	No se realizan revisiones periódicas de ciber seguridad
Medidas Técnicas	Segmentación de red	La segmentación y la segregación física o lógica se implementan en la red ICS. Se utilizan firewall entre la red ICS y la red LAN Corporativa
	Acceso Remoto	Hay definido un procedimiento
	Monitoreo	No existe monitoreo sobre la red ICS
	Métodos de Detección de Intrusiones	No se establecen métodos de detección de intrusos
	Plan de Continuidad del Negocio (BCP)	No existe un BCP
Impacto en el Negocio	Health & Safety (Interno & Externo)	Enfermedad o lesión grave que impacte en días fuera del trabajo; o Invalidez parcial permanente
	Medio Ambiente	Liberación al medio ambiente de sustancias, que generen quejas, olores y/o ruidos molestos
	Financiero	Posibles daños a los activos o pérdida financiera de USD 100 000 a USD 1 millón o más del 10 % del valor total de los activos

Operativo (Capacidad & Duración)	El 10 % de la capacidad instalada no está operativa durante un período de <10 días o 5% de la capacidad instalada no operativa por un período de > 10 días
Legal / Regulaciones	Requiere una investigación por parte de autoridades externas u organismos reguladores.
Reputación	Daño menor a la reputación pública de la Compañía y/o preocupación de los clientes
Propiedad Intelectual	Desventajas competitivas moderadas

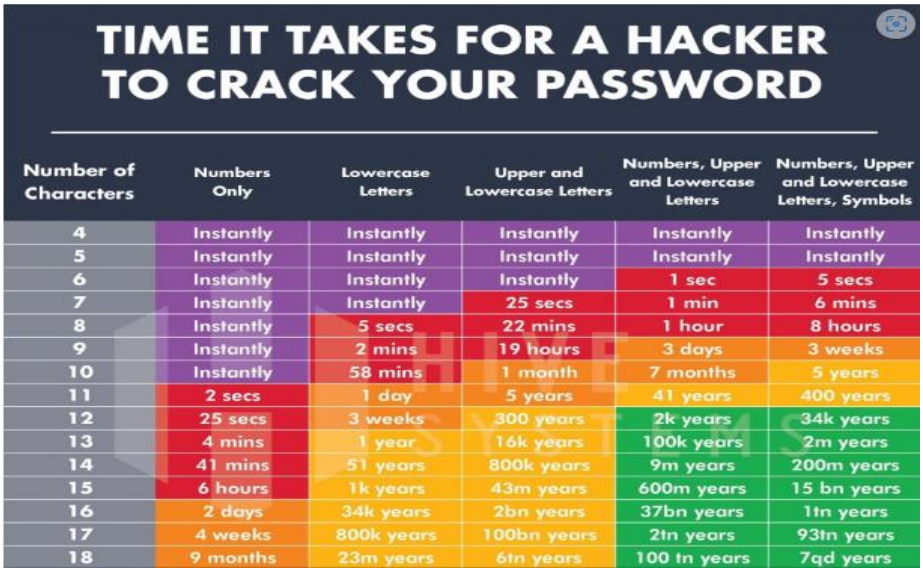
Nota. Extraído del Cuestionario de Estratificación del Riesgo.

Respecto a la conectividad un punto a tener en cuenta es que la red ICS y la red LAN Corporativa están conectadas y separadas mediante un Firewall Fortinet 30F, la gestión de accesos y usuarios, actualmente se utilizan cuentas de usuarios locales y genéricos, sin la aplicación de ninguna política de contraseñas esto se evidencia ante la falta de configuraciones que fuercen el uso de contraseñas con complejidad y frecuencia de cambio de contraseña, tampoco se posee un directorio para la administración y configuración de políticas centralizadas, además los responsables del sector industrial no utilizan un gestor de contraseñas para el resguardo de los usuarios y claves con mayores privilegios, ni procedimientos de políticas de manejo y custodia.

La Figura 23 nos ayuda a comprender el riesgo de utilizar contraseñas débiles y la relación directa en la cantidad de tiempo que un atacante necesita para obtenerla, y como la falta de políticas de contraseñas puede afectar seriamente a una organización.

Figura 22

Tiempo que Demora un Hacker en Obtener tu clave



Nota. Figura extraída del sitio web Locker (Locker, 2022)

En la categoría Gobierno o Governance no existe una definición formal sobre los roles y responsabilidades, tampoco se realizan revisiones anuales de ciberseguridad ni test de penetración, poseen un inventario, pero el mismo no tiene definido los tipos de activos, su nivel riesgo y criticidad. En la sección Medidas Técnicas, observamos que entre ambas redes existe un Firewall Fortinet 30F, hay segmentación física y lógica utilizando VLAN, de sus siglas en inglés "Virtual Local Area Network", para separar las redes, hay definido un procedimiento por el área de IT para dar acceso remoto a los proveedores, que lo gestiona el área de IT mediante la creación de un Ticket de soporte, para conectarse a la VPN se utiliza el cliente de Fortinet, llamado FortiClient, pero no tienen adoptado el uso de MFA, de sus siglas en ingles "Multi Factor Authentication", no hay evidencias de que los distintos niveles de la red industrial sean monitoreados con alguna herramienta que les permita obtener información del estado de salud de todos los componentes de la infraestructura de misión crítica, incluidas las aplicaciones, servicios, sistemas operativos y protocolos de red, pudiendo obtener métricas de los sistemas e infraestructura de la red industrial, tampoco poseen una herramienta para la persistencia de eventos en un SIEM, de sus siglas en ingles "Security Information and Event Management" que permita ante una brecha de seguridad correlacionar los eventos y determinar su origen, no hay definido un procedimiento de respuesta de incidentes que sirva como guía y que establezca los pasos a seguir en caso de que ocurra un evento de ciberseguridad, no se utiliza una herramienta para la detección de intrusos y no existe ningún procedimiento o documento que formalmente explique los pasos del BCP, de sus siglas en inglés "Business Continuity Plan". Por último, el impacto en el negocio de una brecha de seguridad es grande ya que se identifican consecuencias como perdida de días laborales de los empleados, problemas ambientales, financieros desde USD 100.000 a USD1.000.000, reducción en la capacidad de producción con consecuencia de pérdidas de días, acciones legales, daños en la reputación y perdida de ventajas competitivas sobre el resto de los competidores.

Capítulo III

3.1 Resumen

En este capítulo, se expondrán las acciones necesarias para llevar a cabo el diseño de la propuesta.

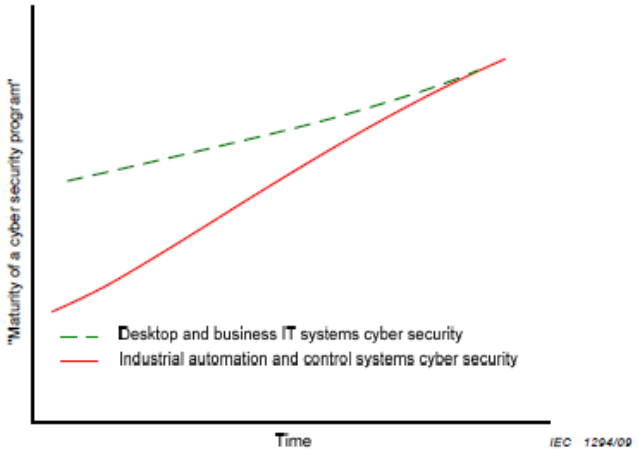
3.2 Propuesta

Para comenzar con el primer objetivo específico se completó el relevamiento de la red industrial de CALSA, esta actividad fue realizada mediante el uso de cuestionarios y entrevistas que permitieron despejar dudas y finalizar el diagnóstico. La propuesta es diseñar un plan de ciberseguridad, que le permita a la organización asegurar los siguientes aspectos básicos: disponibilidad, integridad, confidencialidad y control de acceso. Se debe adoptar un enfoque proactivo, de mejora continua en los procesos y procedimientos, entendiéndose como proceso a un conjunto estructurado de actividades que nos ayudan a cumplir objetivos (van Bon, et al., 2008). La mejora continua es un concepto utilizado en diversos ámbitos, siendo un enfoque sistemático y constante de buscar y aplicar mejoras en una organización, el principal objetivo es impulsar mediante las revisiones el crecimiento, la eficacia, la eficiencia y la calidad a lo largo del tiempo (ISO/IEC 20000, 2018).

La postura de las organizaciones respecto a la ciberseguridad de IT y los entornos industriales históricamente se mantuvieron separadas, el conocimiento y los requerimientos nunca fueron entendidos por las partes involucradas. Cuando las organizaciones intentaron aplicar prácticas de IT en los entornos industriales se presentaron dificultades, entorpeciendo la operación de los entornos industriales. En la Figura 24 podemos visualizar como la integración debe ser una decisión estratégica de la organización para que ambas áreas trabajen en conjunto compartiendo el conocimiento y sus habilidades. El principal objetivo de un plan de ciberseguridad es integrar todos los aspectos, incluyendo los sistemas informáticos de IT y los sistemas de control y automatización industrial, un enfoque errado es creer que se debe afrontar como un típico proyecto que inicia y finaliza, debido a que permanentemente aparecen nuevas amenazas, vulnerabilidades, tecnologías, los atacante mejoran sus técnicas para evitar que sean detectados y generar más daño. (IEC/TS 62443, 2009).

Figura 23

Integración de la ciber seguridad en entornos de IT y IACS



Nota. Figura extraída de la IEC 62443-1-1

El estándar ISA99/IEC 62443 define a una Zona (zone) como la agrupación lógica o física de activos industriales, estos pueden ser elementos físicos, aplicaciones o información, los cuales comparten los mismos requisitos de seguridad, además define el flujo en las comunicaciones que permite que la información y las personas interactúen dentro y entre las zonas de seguridad. Las zonas se pueden definir como zona física, que incluye a los activos físicos dentro de una locación o bien como una zona virtual que abarca a los grupos de activos, partes de activos físicos con una característica en particular. Las zonas pueden considerarse de confianza (trusted) o no confiable (untrusted).

Un Conducto (conduits) es un tipo especial de zona que cubre los aspectos de seguridad en las comunicaciones entre diferentes zonas, para que se realice de forma segura. Al igual que con las zonas, los conductos pueden ser elementos físicos y lógicos. Los conductos pueden considerarse de confianza (trusted) o no confiable (untrusted).

Por último, se agrega el concepto de Canal (channel) el cual es un vínculo de comunicación establecido dentro de un conducto, este hereda los requerimientos de seguridad del conducto. Un canal confiable (trusted) es una enlace de comunicación que permite que la comunicación sea segura con otra zona de seguridad, mientras que un canal no confiable (untrusted) son enlaces de comunicación que no tienen el mismo nivel de seguridad (IEC/TS 62443, 2009).

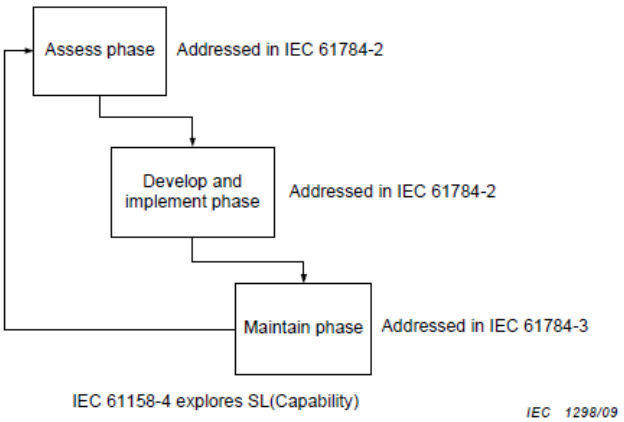
El estándar ISA99/IEC 62443 define el nivel de seguridad (Security Level) como el marco de referencia para la toma de decisiones dependiendo de los dispositivos y acciones

correctivas. Los tipos de niveles de seguridad son 3: SL(Target), es el nivel objetivo, debe ser asignado a las zonas y podría utilizarse en los conductos (conduits), en ambos casos se debe determinar en la evaluación de riesgo, el SL(Target) determinará el tipo de medidas de seguridad que se deberán adoptar, como por ejemplo incorporar firewalls, antivirus, desarrollar políticas y procedimientos, accesos físicos y lógicos. El SL(Achieved), corresponde al nivel logrado, por las propiedades de seguridad inherentes a los dispositivos, sistemas, zonas, conductos y/o medidas de seguridad implementadas, este nivel depende directamente del tiempo que transcurre entre que se aplican las medidas de seguridad, la obsolescencia de los dispositivos y sistemas, las nuevas vulnerabilidades, amenazas y métodos de ataque que surgen. Por último, SL(Capability) es el nivel capacidad que tiene los dispositivos, sistemas, zonas o conductos de adoptar las medidas de seguridad implementadas.

En la Figura 25 podemos observar cómo es el ciclo de vida de los niveles de seguridad, de acuerdo con el estándar ISA99/IEC 62443 aquí se definen las 3 etapas: Evaluación, Desarrollo & Implementación y Mantenimiento. El primer paso es determinar el Sistema bajo consideración (SUC), de sus siglas en ingles “System Under Consideration” que no es otra cosa que la infraestructura que se analizará. En la etapa de Evaluación (Assess Phase) se definen los límites de las zonas, los criterios de aceptación de riesgos de la organización y se asigna el SL(Target). En la etapa de Desarrollo & Implementación se deben implementar las medidas de seguridad que permitirán alcanzar el SL(Achieved). La etapa de Mantenimiento requiere que se realicen auditorias y pruebas ya que las medidas de seguridad adoptadas con el tiempo pueden quedar obsoletas (IEC/TS 62443, 2009).

Figura 24

Ciclo de Vida de los Niveles de Seguridad



Nota. Figura extraída de la IEC 62443-1-1

La Tabla 28 indica los nivel de seguridad sobre los cuales se basará el diseño del plan de ciber seguridad, debido a que la organización no es un objetivo de activistas ni tampoco es parte del estado nacional, se decide diseñar el plan en base a nivel de seguridad SL2.

Tabla 28

Niveles de Seguridad

Nivel de Seguridad	Objetivo	Habilidades	Motivación	Medio	Recursos
SL1	Eventos casuales o accidentales	Sin Habilidades	Ninguna/Error	No intencional	Una persona
SL2	Cyber Delincuentes	Comunes	Baja	Simples	Bajos
SL3	Hackers/Activista Terroristas	Específicas para ICS	Moderada	Sofisticada	Grupos de hackers
SL4	Estado Nacional	Específicas para ICS	Alta	Sofisticada	Externos

Nota. Figura extraída de la IEC 62443-1-1.

Que se adopten programas de ciberseguridad es un cambio cultural dentro de la organización que llevará tiempo y recursos. El plan de ciberseguridad abordará los siguientes puntos:

Evaluación de riesgos: Identificaremos y evaluaremos los riesgos específicos del entorno industrial, se considerará los posibles puntos de entrada de amenazas, las vulnerabilidades en los sistemas existentes y las consecuencias e impactos potenciales de un ataque.

Política de seguridad: Se definirá una política de seguridad clara y documentada que establezca los lineamientos principales para proteger los sistemas industriales, incluirá aspectos como el acceso a los sistemas, la gestión de usuarios tanto operativos como los que tengan altos privilegios, administración de contraseñas, control de dispositivos, uso de antivirus, las actualizaciones de sistemas operativos y software relacionado a los procesos industriales.

Protección de la red: Diseñar una infraestructura de red segura, confiable y escalable, se considerará la segmentación de la red para aislar los sistemas críticos, la implementación de firewalls, MFA, sistemas de detección y prevención de intrusiones (IDS/IPS).

Protección de sistemas: Se definirán medidas de seguridad específicas para los sistemas industriales, como los PLC y SCADA, considerando la aplicación de actualizaciones y acciones correctivas, siempre que las características de los sistemas lo permitan.

Concientización y capacitación: Se deberá fomentar en la organización una cultura de ciberseguridad. La educación y capacitación es uno de los pilares y debe ser considerado estratégico. Se definirán planes de capacitación que contemplen las mejores prácticas de seguridad, reconocer amenazas y qué hacer en caso de incidentes, estos planes de formación y concientización serán orientados para que los colaboradores relacionados con él área industrial, les permita comprender la tecnología de la información vigente, se deberá incluir al personal de TI para que aprendan sobre las tecnologías de los ICS, junto con la seguridad del proceso y métodos de gestión. Desarrollar prácticas que integren a toda la organización para afrontar la ciberseguridad en colaboración y acciones para que todos los actores entiendan los riesgos, roles y responsabilidades.

Respaldo y recuperación de datos: Se definirá e implementará una política de Backup con procedimientos regulares de respaldo de datos y sistemas estableciendo un plan de recuperación en caso de un ataque o desastre. Dicha política deberá asegurar que los datos críticos estén respaldados y que se puedan restaurar rápidamente en caso de pérdida. Se deberá trabajar en definir el RPO, RTO, WRT y MTD. El RPO, de sus siglas en inglés “Recovery Point Objective”, que es la cantidad máxima de pérdidas de datos aceptada por la organización. También se acordará el RTO, de sus siglas en inglés “Recovery Time Objective”, aquí se especificará cual es el tiempo máximo que la organización tolera hasta tener todos los sistemas en línea. Sobre el WRT, de sus siglas en inglés “Working Recovery Time”, es el tiempo máximo tolerable por la organización que es necesario para verificar los sistemas. Y finalmente el MTD, de sus siglas en inglés “Maximun Tolereable Downtime”, es el tiempo máximo de interrupción tolerable sin tener consecuencias inaceptables para la organización.

Monitoreo: Se implementará un sistemas de monitoreo para detectar caídas de los servicios críticos industriales definiendo un esquema de notificación a los responsables.

Respuesta ante incidentes: Se definirá un proceso claro para notificar, comunicar y responder a los incidentes de seguridad, incluyendo la investigación, la mitigación y el seguimiento de las lecciones aprendidas.

Evaluación y mejora continua: Se redactará un procedimiento para realizar al menos 1 vez al año evaluaciones periódicas de la seguridad, identificando posibles brechas de seguridad

y áreas de mejora. A medida que evolucionan las amenazas y las técnicas de ataque, es importante mantenerse actualizado y realizar los ajustes correspondientes.

3.3 Resultados

Diseñar el plan de ciberseguridad utilizando como guía el estándar IEC 62443, incorporando los puntos mencionados en la sección anterior.

3.4 Plazos y cronogramas

En la Figura 26 se estima el desarrollo del plan de ciberseguridad, las tareas, el tiempo estimado por cada una y sus responsables. La duración estimada del proyecto es de 9 meses. El cronograma es expresado en 5 fases las cuales son: Inicio y Planificación, Relevamiento, Diseño del Plan de Ciberseguridad, Implementación del Plan y Cierre el Proyecto. Las tareas están estimadas en semanas laborales de lunes a viernes de 9 a 18 horas. Se estima los recursos humanos involucrados para el proyecto.

Figura 25

Estimación de las Tareas a Realizar

Actividades	Responsable	Mes	1				2				3				4				5				6				7				8				9			
		Semanas	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Fase 1: Inicio y Planificación																																						
Planificación	Lider del Proyecto																																					
Elaboración del Plan del Proyecto	Lider del Proyecto																																					
Elaboración del documento del Plan del Proyecto	Lider del Proyecto																																					
Cronograma	Lider del Proyecto																																					
Fase 2: Relevamiento																																						
Relevamiento de los sistemas industriales	Analista de Ciberseguridad																																					
Diagrama de la Topología y conexiones	Analista de Ciberseguridad																																					
Inventario de Activos	Analista de Ciberseguridad																																					
Identificación de Riesgos	Analista de Ciberseguridad																																					
Auditoria de equipamiento	Analista de Ciberseguridad																																					
Revision de configuracion de Seguridad	Analista de Ciberseguridad																																					
Evaluación de Vulnerabilidades del sistema	Analista de Ciberseguridad																																					
Relevamiento de las redes	Analista de Ciberseguridad																																					
Informe del relevamiento	Analista de Ciberseguridad																																					
Fase 3: Diseño del Plan de CiberSeguridad																																						
Evaluación de riesgos	Analista de Ciberseguridad																																					
Política de seguridad	Analista de Ciberseguridad																																					
Protección de la red	Analista de Ciberseguridad																																					
Protección de sistemas	Analista de Ciberseguridad																																					
Concientización y capacitación	Analista de Ciberseguridad																																					
Respaldo y recuperación de datos	Analista de Ciberseguridad																																					
Monitoreo	Analista de Ciberseguridad																																					
Respuesta ante incidentes	Analista de Ciberseguridad																																					
Evaluación y mejora continua	Analista de Ciberseguridad																																					
Fase 4: Implementación del Plan de CiberSeguridad																																						
Política de seguridad	A. de Ciberseguridad/Calsa																																					
Protección de la red	A. de Ciberseguridad/Calsa																																					
Protección de sistemas	A. de Ciberseguridad/Calsa																																					
Concientización y capacitación	A. de Ciberseguridad/Calsa																																					
Respaldo y recuperación de datos	A. de Ciberseguridad/Calsa																																					
Monitoreo	A. de Ciberseguridad/Calsa																																					
Respuesta ante incidentes	A. de Ciberseguridad/Calsa																																					
Evaluación y mejora continua	A. de Ciberseguridad/Calsa																																					
Fase 5: Cierre del Proyecto																																						
Elaboración de Documentacion del Proyecto	A. de Ciberseguridad/Calsa																																					
Reunión de cierre	A. de Ciberseguridad/Calsa																																					

Nota. De Elaboración Propia en base al Plan del Proyecto

3.5 Recursos Necesarios

Para avanzar en el desarrollo del diseño de la propuesta, disponemos de la estructura y materiales necesarios para llevarlo a cabo. Se firmará un acuerdo de confidencialidad entre las partes con el fin de resguardar aspectos legales, proporcionar accesos, permisos y consentimiento de la organización para obtener y analizar la información proporcionada.

3.6 Recursos Materiales

La organización cuenta con los recursos materiales necesarios para llevar a cabo este proyecto, entre ellos se dispondrá de una oficina física en la Planta de Lanús, Notebooks para las personas que participarán en el proyecto, conexión a la red, navegación a internet y acceso al Share Point Online para el resguardo de la documentación correspondiente.

3.7 Recursos Humanos

En esta sección se especificarán los perfiles necesarios para llevar adelante el proyecto.

3.7.1 Perfiles necesarios

A continuación, en la Tabla 29 definimos los perfiles de los recursos humanos necesarios para realizar con éxito este proyecto.

Tabla 29

Perfiles Necesarios para el Proyecto

Perfil	Descripción
Líder del Proyecto	Responsable de estimar, dirigir, coordinar y controlar todas las actividades y los recursos humanos y materiales.
Analistas de Ciberseguridad SR	Encargados de realizar el relevamiento, análisis, definir el plan.
Analistas de Ciberseguridad Semi SR	Encargados de realizar el relevamiento, análisis, definir el plan.
Responsable de ICS - Calsa	Responsable por parte de la organización en proveer los accesos a la información, revisiones y aceptación de las propuestas.
Sponsor	VP Regional de Manufactura

Nota. De elaboración propia en base al Plan del Proyecto

Capítulo IV

4.1 Conclusiones y sugerencias

La industria en general se enfrenta a cambios drásticos debido al número creciente de ataques dirigidos a las infraestructuras críticas, los activos de las organizaciones siguen siendo los elementos más importantes para proteger. Los atacantes y sus métodos crecen constantemente en números y sofisticación, obligando a las organizaciones a estar preparadas e invertir y destinar recursos a detectar y mitigar estas amenazadas.

El principal objetivo de esta propuesta de intervención en el campo profesional es diseñar un plan de ciberseguridad utilizando como guía el estándar IEC 62443. En la actualidad la empresa CALSA no posee un área dedicada a la ciberseguridad en el entorno industrial, el personal que da soporte al entorno industrial carece de conocimientos técnicos adecuados para poder realizar estas tareas e implementar las mejoras necesarias, no cuenta con recursos idóneos para las tareas relacionadas con el Governance que le permita la confección de procedimientos y políticas para abordar el tema de una manera confiable. La seguridad en los ambientes informáticos debe ser una responsabilidad de todos los miembros de la organización sin importar la jerarquía, para que la implementación del plan de ciberseguridad sea exitosa deberá ser impulsado por un cambio cultural dentro de la organización de forma TOPDOWN.

Luego de analizar la información y realizar el diagnóstico, nuestra propuesta es adoptar un plan de ciberseguridad para mejorar la seguridad del área industrial de la empresa CALSA, que incluirá los siguientes puntos:

Evaluación de riesgos e identificación de activos críticos.

Governance, gestión de la documentación, confección de nuevas políticas de seguridad y procedimientos que le permitirá proteger los sistemas industriales.

Protección de la red, el objetivo final es una infraestructura de red segura, confiable y escalable, se considerará la segmentación de la red para aislar los sistemas críticos.

Protección de sistemas, generará medidas de seguridad específicas para los sistemas industriales, como los PLC y SCADA.

Concientización y capacitación, permitirá fomentar dentro de la organización una cultura de ciberseguridad, desarrollar prácticas que integren a toda la organización para afrontarlo de manera colaborativa, generando conciencia de todos los actores para que

comprendan los riesgos, roles y responsabilidades. La educación y capacitación debe ser considerado un pilar estratégico para lograr el éxito. Se definirán planes de capacitación que contemplen las mejores prácticas de seguridad, serán orientados para que los colaboradores relacionados con él área industrial e IT.

Respaldo y recuperación de datos, se definirá e implementará una política de Backup y recuperación acorde a las exigencias del negocio.

Monitoreo, se implementará un sistemas de monitoreo para detectar caídas de los servicios críticos industriales definiendo un esquema de notificación a los responsables.

Respuesta ante incidentes, se confeccionará un proceso claro para notificar, comunicar y responder a los incidentes de seguridad, incluyendo la investigación forense, la mitigación y el seguimiento de las lecciones aprendidas.

Evaluación y mejora continua, implicará revisiones anuales, e incorporar los procesos a revisar en un plan de mejora continua.

Las limitaciones que identificamos son la falta de personal técnicamente capacitado en seguridad de la información, disponibilidad de recursos humanos para llevar a cabo las mejoras planteadas y que la empresa CALSA no reconozca los riesgos asociados y sus consecuencias. Consideramos que la propuesta es superadora respecto a la situación actual y que le permitirá a la empresa CALSA mejorar la seguridad, reducir los riesgos residuales, controlar vulnerabilidades existentes, haciendo que sea un caso de éxito para el resto de las operaciones de la región y del grupo a nivel mundial.

4.2 Trabajos futuros

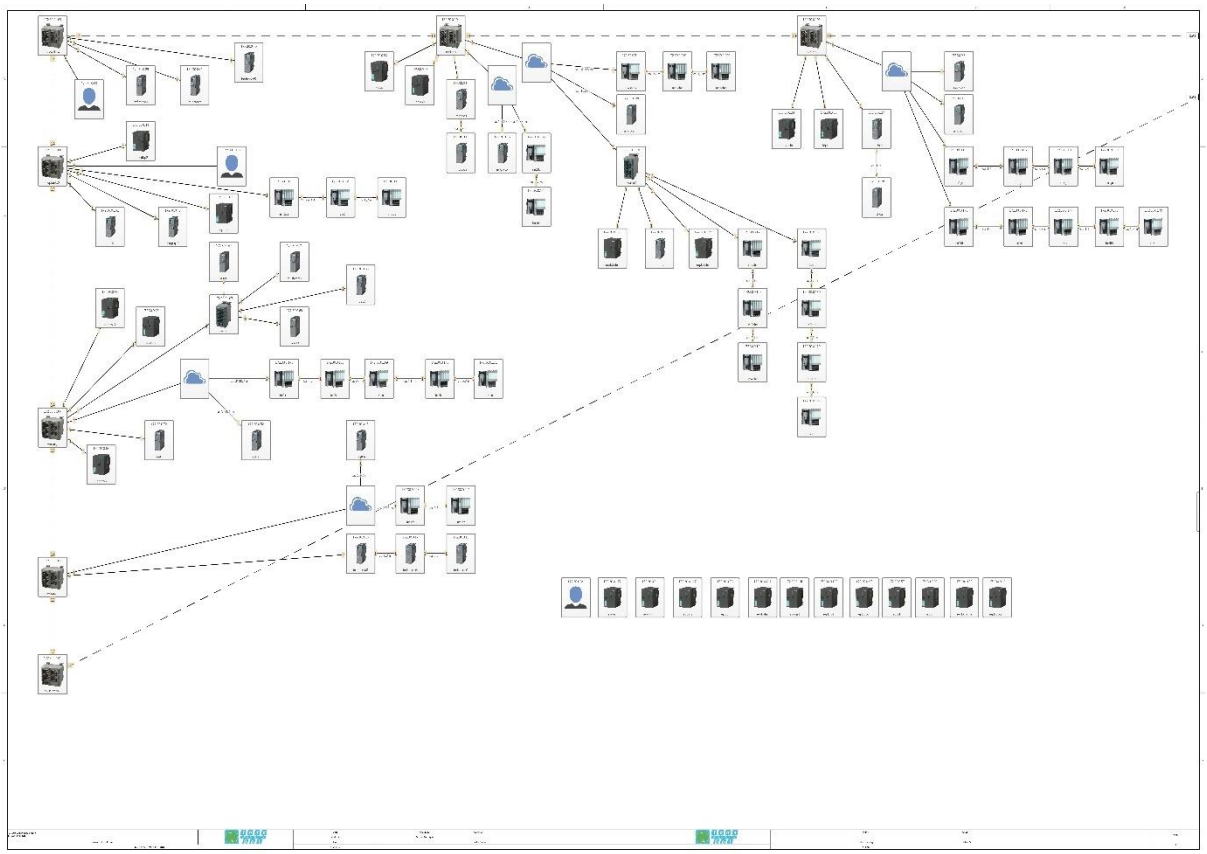
Durante el desarrollo de este documento surgieron nuevas posibilidades que serán utilizadas como líneas futuras de trabajo.

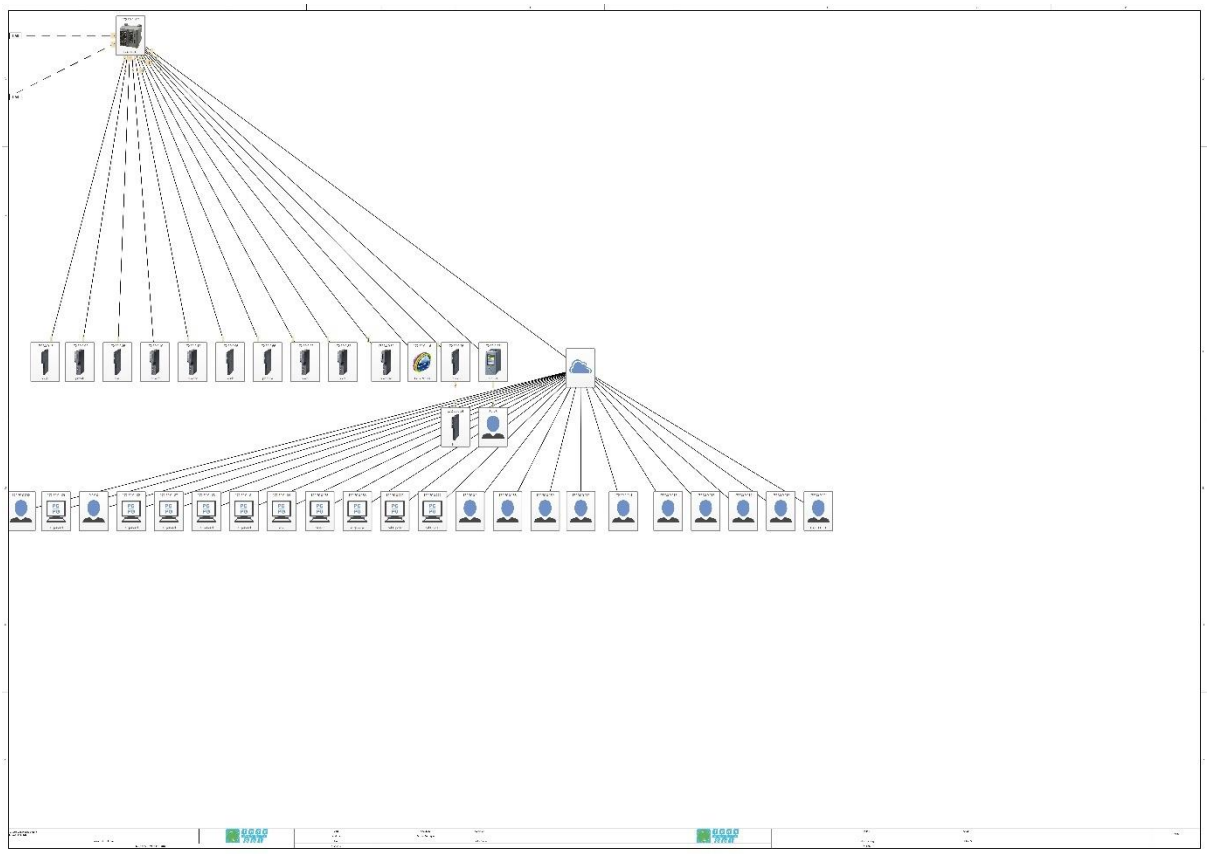
Una vez que CALSA adopte el plan de ciberseguridad en la planta de grasos y margarinas, sugerimos aplicar el mismo criterio, metodología y plan como base para las plantas restantes que la empresa posee en Chile, Ecuador, Uruguay, Perú, Colombia y en la provincia de Tucumán en Argentina. Se deberá relevar cada planta para poder identificar los activos críticos y sus riesgos asociados.

Se sugiere realizar las inversiones necesarias para actualizar los sistemas industriales a las versiones más recientes de sus fabricantes reduciendo de forma considerable las vulnerabilidades presentes por la infraestructura instalada, explorando la tecnología de Cloud Computing para entornos industriales.

Anexo 1

1. Topología

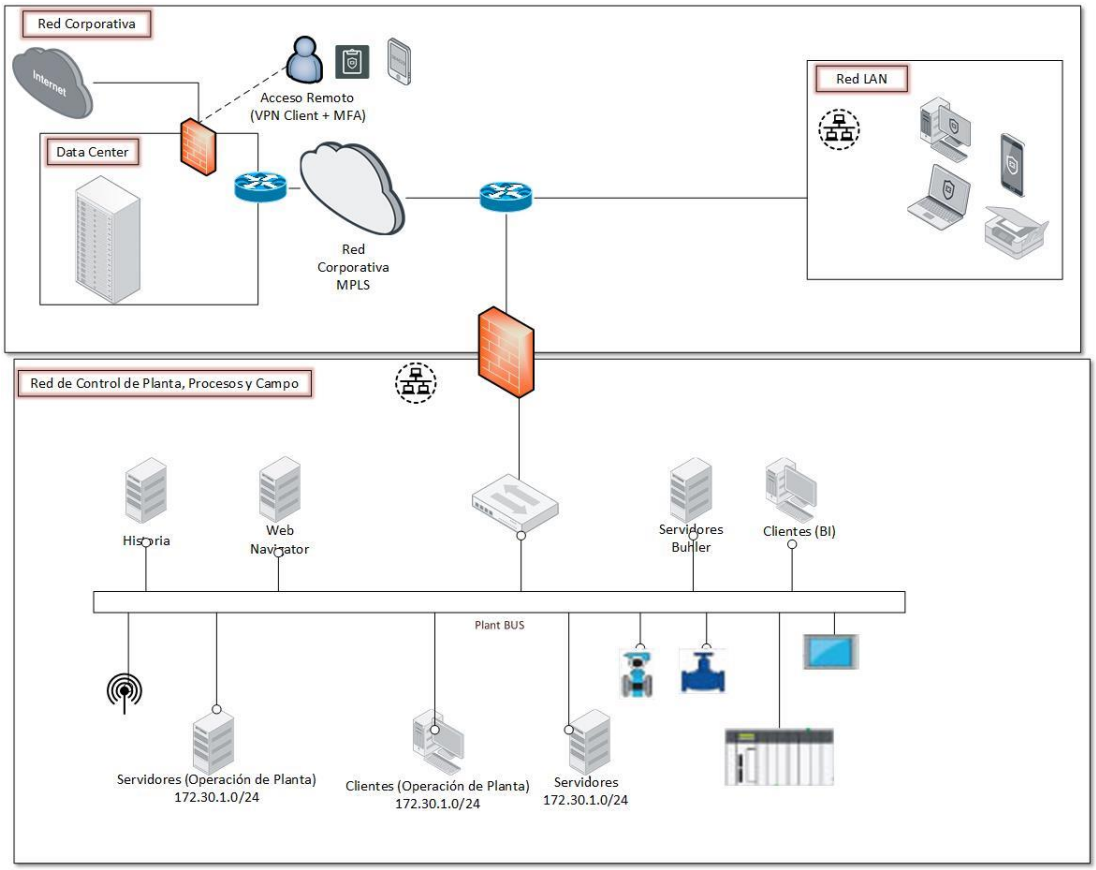




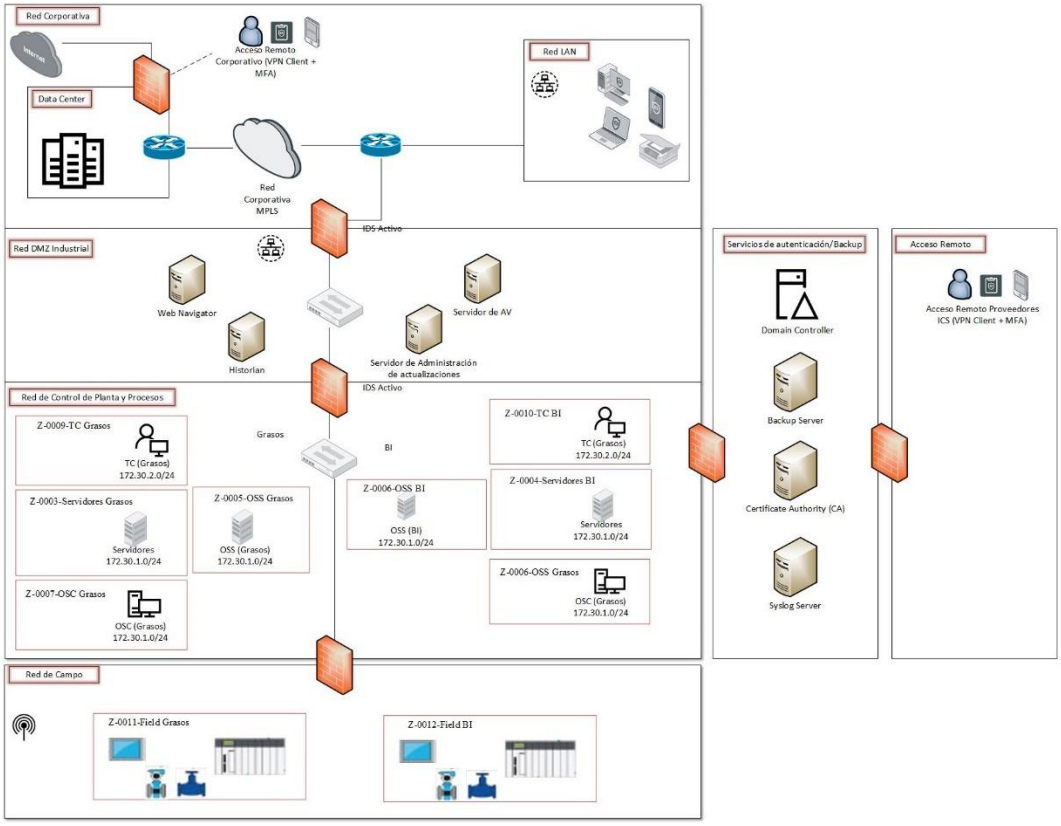
2. Plan del Proyecto

Actividades	Responsable	Mes	1				2				3				4				5				6				7				8				9			
		Semanas	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Fase 1: Inicio y Planificación																																						
Planificación	Lider del Proyecto																																					
Elaboración del Plan del Proyecto	Lider del Proyecto																																					
Elaboración del documento del Plan del Proyecto	Lider del Proyecto																																					
Cronograma	Lider del Proyecto																																					
Fase 2: Relevamiento																																						
Relevamiento de los sistemas industriales	Analista de Ciberseguridad																																					
Diagrama de la Topología y conexiones	Analista de Ciberseguridad																																					
Inventario de Activos	Analista de Ciberseguridad																																					
Identificación de Riesgos	Analista de Ciberseguridad																																					
Auditoria de equipamiento	Analista de Ciberseguridad																																					
Revision de configuracion de Seguridad	Analista de Ciberseguridad																																					
Evaluación de Vulnerabilidades del sistema	Analista de Ciberseguridad																																					
Relevamiento de las redes	Analista de Ciberseguridad																																					
Informe del relevamiento	Analista de Ciberseguridad																																					
Fase 3: Diseño del Plan de CiberSeguridad																																						
Evaluación de riesgos	Analista de Ciberseguridad																																					
Política de seguridad	Analista de Ciberseguridad																																					
Protección de la red	Analista de Ciberseguridad																																					
Protección de sistemas	Analista de Ciberseguridad																																					
Concientización y capacitación	Analista de Ciberseguridad																																					
Respaldo y recuperación de datos	Analista de Ciberseguridad																																					
Monitoreo	Analista de Ciberseguridad																																					
Respuesta ante incidentes	Analista de Ciberseguridad																																					
Evaluación y mejora continua	Analista de Ciberseguridad																																					
Fase 4: Implementación del Plan de CiberSeguridad																																						
Política de seguridad	A. de Ciberseguridad/Calsa																																					
Protección de la red	A. de Ciberseguridad/Calsa																																					
Protección de sistemas	A. de Ciberseguridad/Calsa																																					
Concientización y capacitación	A. de Ciberseguridad/Calsa																																					
Respaldo y recuperación de datos	A. de Ciberseguridad/Calsa																																					
Monitoreo	A. de Ciberseguridad/Calsa																																					
Respuesta ante incidentes	A. de Ciberseguridad/Calsa																																					
Evaluación y mejora continua	A. de Ciberseguridad/Calsa																																					
Fase 5: Cierre del Proyecto																																						
Elaboración de Documentacion del Proyecto	A. de Ciberseguridad/Calsa																																					
Reunión de cierre	A. de Ciberseguridad/Calsa																																					

3. Diagrama de Topología Actual



4. Diagrama de Topología propuesta



Acrónimos

SCADA	Supervisory Control And Data Acquisition
PLC	Programmable Logic Controllers
HMI	Human Machine Interface
NIST	National Institute of Standard and Technology
CSIRT	Computer Security Incident Response Team
IT	Information Technology
IEC 62443	International Electronic Commission 62443
DCS	Distributed Control Systems
RTU	Remote terminal Units
SIS	Safety-Instrumented System
CIA	Confidentiality, Integrity and Availability
ERP	Enterprise Resource Planning
LUN	Logical Unit Number
IDS	Intrusion Detection System
SIEM	Security Information and Event Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
BCP	Business Continuity Plan
IACS	Industrial Automation and Control Systems
RDP	Remote Desktop Protocol
RPO	Recovery Point Objective
RTO	Recovery Time Objective
WRT	Working Recovery Time
MTD	Maximun Tolereable Downtime

Referencias

Alcaraz, C., Fernandez, G., Román, R., Balastegui,, Á., & López, J. (2008). *Gestión segura de redesSCADA, Nuevas tendencias engestión de redes.*

CALSA, Cia Argentina de Levaduras. (s.f.). *CALSA, Cia Argentina de Levaduras*.

Centro de Ciberseguridad Industrial. (s.f.). *Centro de Ciberseguridad Industrial. Actores de la Smart OT.*

Centro de Ciberseguridad Industrial. (s.f.). *Guía de Bolsillo. Ciberseguridad en la pirámide de automatización industrial*.

Cepal. (2019). *La revolución industrial 4.0 y el advenimiento de una logística 4.0.* ISSN: 1564-4227.

Chaves Palacios, J. (2004). Desarrollo tecnológico en la primera revolución industrial. *Norba, Revista de Historia*.

Chiavenato, I. (2007). *Administración de recursos humanos, el capital humano de las organizaciones.* Mc Graw Hill.

Cisco Systems. (s.f.). *Deploying CIP Security within a Converged Plantwide Ethernet.* Obtenido de https://www.cisco.com/: https://www.cisco.com/c/en/us/solutions/design-zone/industries/manufacturing/cpwe.html

Diseño de zonas, conductos y canales, según la normativa IEC 62443 (ISA99) en una industria 4.0. (5 de 10 de 2016). Obtenido de https://isa-spain.org/: https://isa-spain.org/diseno-de-zonas-conductos-y-canales-segun-la-normativa-iec-62443-isa99-en-una-industria-4-0-i/?cn-reloaded=1

Eset. (2021). *Security Report - Latinoamérica.*

Eset. (2022). *Security Report - Latinoamérica.*

Gobierno de la República Argentina. (28 de 05 de 2019). *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD - APROBACION.* Obtenido de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-829-2019-323594/texto

https://www.fortinet.com/lat. (Mayo de 2023).

https://www.nagios.com/. (Mayo de 2023).

IEC/TS 62443. (2009). *IEC/TS 62443-1-1,Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models.*

Informe anual del CERT.ar. (22 de 02 de 2022). *Informe anual del CERT.ar.*

ISA. (s.f.). *ISA.*

ISO/IEC 20000. (2018). *ISO/IEC 20000-1:2018, Information technology — Service management.*

ISO/IEC 27000:2018. (2018). *ISO/IEC 27000:2018. Tecnología de la información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información.*

Kapersky. (2019). *Threat landscape for industrial automation systems.*

Kaspersky. (2021). *Threat landscape for industrial automation systems.* Obtenido de https://ics-cert. kaspersky.com/reports/2020/09/24/threat-landscapefor-industrial-automation-systems-h1-2020

Landes, D. (1979). *Progreso tecnológico y revolución industrial.* Madrid: Tecnos.

Locker. (27 de Septiembre de 2022). *Locker.*

Meyer, N. (2017). *The German Standardization System and Industry 4.0: An institutional analysis.*

Ministerio de Modernización. (s.f de s.f de s.f). *El panorama de la ciberseguridad en números.*

Observatorio de la Ciberseguridad en América Latina y el Caribe. (Mayo de 2023). *Observatorio de la Ciberseguridad en América Latina y el Caribe*.

Rifkin, J. (2011). *La tercera revolución industrial.* Paidos.
Rojko, A. (24 de 07 de 2017). *International Journal of Interactive Mobile Technologies.* https://doi.org/https://doi.org/10.3991/ijim.v11i5.7072
Security, IBM. (2022). *Informe del Coste de la vulneración de datos.*
Siemens, SCALANCE. (s.f.). *Siemens, SCALANCE – network components for industrial communication*.
The Cyber Security Body of Knowledge. (31 de Octubre de 2019). Obtenido de https://www:cybok:org/
van Bon, J., de Jong, A., Kolthof, A., Pieper, M., T'jassing, R., van der Veen, A., & Verheijen, T. (2008). *Fundamentos de ITIL V3.* Van Haren Publishing, Zaltbommel.
Verizon. (2022). *Verizon Data Breach Investigations Report.*