



TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE APIZACO

NOMBRE DEL PROYECTO

IMPLEMENTACIÓN DE RESILIENCIA APLICADA LAS MEJORAS DE SEGURIDAD PARA LA INFRAESTRUCTURA TI EN SCHNEIDER ELECTRIC PLANTA TLAXCALA.

OPCIÓN

TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACIÓN.

PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

PRESENTA:

GUADALUPE RAMOS SERRANO

ASESOR INTERNO:

M.C. NICOLÁS ALONZO GUTIÉRREZ

ASESOR EXTERNO:

ING. FAUSTO DÍAZ SANTILLÁN



APIZACO, TLAX., JUNIO, 2025.

Apizaco, Tlaxcala, 29/noviembre/2024

Oficio No. S.C./OPV/0266/2024

Asunto: Liberación de proyecto para titulación.

ISRAEL SÁNCHEZ SÁNCHEZ
JEFE DEL DEPTO. DE DIVISIÓN DE ESTUDIOS PROFESIONALES
PRESENTE

POR ESTE MEDIO LE INFORMO QUE HA SIDO LIBERADO EL SIGUIENTE PROYECTO PARA TITULACIÓN.

NOMBRE DEL EGRESADO:	GUADALUPE RAMOS SERRANO
CARRERA:	INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
NO. DE CONTROL:	13370823
NOMBRE DEL PROYECTO:	IMPLEMENTACIÓN DE RESILIENCIA APLICADA A LAS MEJORAS DE SEGURIDAD PARA LA INFRAESTRUCTURA TI EN SCHNEIDER ELECTRIC PLANTA TLAXCALA
PRODUCTO U OPCIÓN:	OPCIÓN III. PROYECTO DE INVESTIGACIÓN

AGRADEZCO DE ANTEMANO SU VALIOSO APOYO EN ESTA IMPORTANTE ACTIVIDAD PARA LA FORMACIÓN PROFESIONAL DE NUESTROS EGRESADOS.

ATENTAMENTE
Excelencia en Educación Tecnológica
Pensar para Servir, Servir para Triunfar



JOSÉ ANTONIO CUATEPOTZO VARELA
JEFE DEL DEPTO. DE SISTEMAS Y COMPUTACIÓN

SECRETARÍA DE EDUCACIÓN PÚBLICA
TECNOLÓGICO NACIONAL
DE MÉXICO

 NICOLÁS ALONZO GUTIÉRREZ	 JOEL GÓMEZ QUINTERO	 MERCED PÉREZ MORENO
NOMBRE Y FIRMA DEL ASESOR	NOMBRE Y FIRMA DEL REVISOR	NOMBRE Y FIRMA DEL REVISOR

ccp. Coordinación de carrera
Expediente

JACV/mrol*





Educación
Secretaría de Educación Pública



TECNOLÓGICO
NACIONAL DE MÉXICO



Instituto Tecnológico de Apizaco
División de Estudios Profesionales

Tzompantepec, Tlaxcala, **10/junio/2025**

RAMOS SERRANO GUADALUPE
EGRESADO(A) DE LA CARRERA INGENIERÍA
EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.
CON NÚMERO DE CONTROL 13370823.
P R E S E N T E.

Por este medio, me permito informar a usted que por aprobación de la comisión revisora asignada para valorar el trabajo que mediante la opción TITULACIÓN INTEGRAL PROYECTO DE INVESTIGACIÓN y cuyo tema es: IMPLEMENTACIÓN DE RESILIENCIA APLICADA A LAS MEJORAS DE SEGURIDAD PARA LA INFRAESTRUCTURA TI EN SCHNEIDER ELECTRIC PLANTA TLAXCALA, conforme a lo establecido en el procedimiento para la obtención del Título Profesional en el Instituto Tecnológico, la División de Estudios Profesionales a mi cargo le otorga la:

AUTORIZACIÓN DE IMPRESIÓN

Debiendo entregar 2 USB del mismo, apropiadamente empastados, a la brevedad, para presentar su Acto de Recepción Profesional.

Sin otro particular por el momento me despido.

ATENTAMENTE

Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®



SECRETARÍA DE EDUCACIÓN PÚBLICA
TECNOLÓGICO NACIONAL
DE MÉXICO
INSTITUTO TECNOLÓGICO DE APIZACO
DIVISIÓN DE
ESTUDIOS PROFESIONALES

ISRAEL JORGE SÁNCHEZ SÁNCHEZ
JEFE DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES

ccp. Archivo
IJSS/rrc



2025
Año de
La Mujer
Indígena

Av. Instituto Tecnológico No. 418, San Andrés Ahuashuatepec,
Municipio de Tzompantepec, Tlaxcala, Mex. C.P. 90491 Tel. (241) 4172010
Ext. 304, e-mail: dep_titulacion@apizaco.tecnm.mx | apizaco.tecnm.mx



Agradecimientos

En primer lugar, quiero expresar mi más sincero amor y agradecimiento a Dios, el padre azul, porque cada mañana me bendice con un nuevo comienzo, aunque no sea merecedora de ello. Le doy gracias a Dios por darme paciencia, llenarme de fortaleza y brindarme entendimiento para alcanzar mis objetivos. Agradezco al señor, ya que con el mismo significado que lleva este proyecto, me ha convertido en una mujer RESILIENTE.

Quiero dedicar este proyecto a la memoria de mi padre José Ramos, a quien amo con todo el corazón. Aunque ya no está físicamente conmigo, sigue siendo una fuente de inspiración y fortaleza en mi vida. Él personificaba todo lo que significa la palabra RESILIENCIA. Su ejemplo de perseverancia, dedicación y amor incondicional ha sido el pilar que me ha sostenido a lo largo de este camino. A él, que siempre creyó en mis capacidades y me enseñó el valor del esfuerzo, le debo gran parte de este logro. A mi papillo millo, gracias por guiarme con tu sabiduría y por ser mi modelo a seguir. Todo lo que logre en esta vida será tanto mío como tuyo.

A mi madre, no hay palabras suficientes para expresar toda mi gratitud, pero quiero intentarlo en este breve espacio. Gracias por tu amor incondicional, por enseñarme a ser madre en medio de las tormentas, incluso cuando yo misma dudaba de mis capacidades. Has sido mi ejemplo de fortaleza y entrega, y me has inculcado valores que me han llenado de sabiduría. Gracias por exhortarme siempre a dar lo mejor de mí como mujer y como madre. Tus lecciones han sido una brújula en los momentos más difíciles.

A mi hijo Ángel Gael, mi mayor fuente de motivación y alegría. Gracias por tu paciencia y comprensión durante los momentos en que tuve que dedicarme intensamente a mis estudios y, ahora, a mi vida laboral. Tu presencia, tu sonrisa y tu amor me han dado la fuerza para seguir adelante, incluso en los momentos más difíciles. Quiero recordarte que la vida no es fácil, pero espero que este logro te inspire a seguir tus propios sueños con pasión y determinación.

Al Ingeniero Fausto Díaz Santillán, quiero expresarle mi más sincero agradecimiento por darme la oportunidad de formar parte de su equipo y por su apoyo constante durante este proceso. Gracias por creer en mis capacidades, por tu paciencia y, sobre todo, por tu confianza. Agradezco el haber creado un entorno de aprendizaje continuo que me permitió desarrollarme de manera profesional y laboral.

Finalmente, quiero agradecer a todos mis profesores. Su guía y apoyo han sido fundamentales en este proceso. En especial a mi asesor, al M.C. Nicolás Alonzo Gutiérrez, con quien tuve el honor de tomar clases. Gracias por compartir su conocimiento y experiencia.

A todos ustedes, gracias por su amor, apoyo y guía. Este logro no hubiera sido posible sin cada uno de ustedes.

Resumen

En el presente trabajo se exponen los procesos que respaldan la continuidad del negocio en el sector eléctrico industrial, específicamente en Schneider Electric, Planta Tlaxcala (SE). La seguridad y la automatización juegan un papel crucial en el cumplimiento de los objetivos de la planta a nivel local, alineándose también con la misión general de la organización. Esto se debe a que la tecnología se ha transformado y en función de ello de la misma forma sigue transformando los procesos comerciales que respaldan los servicios necesarios para alcanzar las metas de la entidad. El enfoque de este trabajo está en el respaldo de los servicios tecnológicos de TI, específicamente en el cuidado de su infraestructura física mediante la integración de dispositivos inteligentes, como la implementación de hardware. La industria debe ser capaz de adaptarse a los cambios del entorno, por lo que aquí se describe la gestión, implementación y desarrollo de nuevas estrategias para mejorar la infraestructura. Esto se logra a través de una metodología y un marco referencial que fomentan la resiliencia tecnológica, el primer paso para mitigar los problemas de seguridad en la infraestructura física dentro de la planta. El trabajo también hace referencia a la infraestructura actual y cómo se ha intervenido mediante la implementación de sistemas como vigilancia física, controles de acceso, sensores de temperatura y sistemas de alimentación ininterrumpida. De esta manera, se abarcan las innovaciones, actualizaciones e implementaciones de hardware necesarias. La resiliencia en TI es una parte fundamental de este proyecto, cuyo objetivo general es cuidar y proteger la infraestructura tecnológica, fortaleciéndola y asegurando la salvaguarda de información crítica. El propósito principal es promover buenas prácticas que permitan a la industria generar procesos operativos más eficientes mediante la automatización. Al mejorar todos los aspectos de su negocio, la organización puede evitar el estancamiento en situaciones de crisis derivadas de fallas en la seguridad de la infraestructura física de TI.

ÍNDICE

CONTEXTO GENERAL DEL PROYECTO	1
Introducción	1
Planteamiento del problema	3
Justificación	4
Objetivos.....	4
General.....	4
Específicos.....	4
Alcances.....	5
Limitaciones	5
FUNDAMENTOS TEÓRICOS	7
Marco Teórico	7
El propósito de una resiliencia en la industria	8
MÉTODO ESTRATÉGICO PARA LA IMPLEMENTACIÓN DEL PROYECTO	11
Metodología.....	11
ANÁLISIS Y DESARROLLO	14
Plan de acciones para establecer la resiliencia	14
Liderazgo	15
La disciplinariedad de ser organizado	15
La flexibilidad.....	15
Preparación y planificación	15
La resiliencia a través de una cultura.....	15
Identificación de la infraestructura física interna y descripción general de requerimientos	19
Identificación de IDFs en planta.....	25
El IDF y su funcionamiento descriptivo.....	32
El funcionamiento de la seguridad operativa en el hardware.....	33
Acceso físico.....	34
Desastres naturales	34
Evaluación de la comprensión a la exposición al riesgo	34
El desfase del hardware en la infraestructura	35
Principios de reducción a los riesgos.....	35

Requerimientos para la mejora del servicio TI en infraestructura.....	36
Procesos de gestión de resiliencia en la infraestructura TI.....	37
Gestión de la seguridad.....	37
Gestión de la continuidad del negocio.....	37
Gestión de la operación de TI.....	38
Estándares de normatividades de la continuidad empresarial	39
ISO 22301 (Plan de continuidad de negocio).....	39
ISO 27031 (Preparación de las organizaciones ante incidentes de interrupción de los servicios de tecnología de la información TI)	40
Proceso de resiliencia en infraestructura TI basados en los dispositivos automatizados	41
IMPLEMENTACIÓN TECNOLÓGICA	45
Descripción inicial de los dispositivos	45
NetBotz Room Monitor 750	45
NetBotz Wall Monitor 755	47
Fase inicial primaria instalación de hardware al centro de datos	49
Configuración inicial realizada por el socio técnico (tech partner) a través de una computadora .	50
Fase secundaria instalación de monitor de sala NetBotz 755 en IDFs	56
IMPACTO Y RESULTADO	62
Pruebas de funcionalidad y rendimiento	62
Mejoras en la resiliencia	66
Conclusiones	68
Referencias	69

ÍNDICE DE FIGURAS Y TABLAS

Figura 1 Factores para lograr la resiliencia organizacional.	14
Figura 2 Aspectos de gestión para la continuidad del proceso de resiliencia.	16
Figura 3 Cronograma de actividades.....	17
Figura 4 Requerimientos de la infraestructura física interna.	18
Figura 5 Layout (Diseño interno, y distribución visual de la planta).....	19
Figura 6 implementaciones para los sistemas de comunicación.	20
Figura 7 Principal Centro de Datos de SE Planta Tlaxcala.....	21
Figura 8 Racks internos del Centro de Datos.	22
Figura 9 RACKS del centro de datos con deficiencia de seguridad en chapas y monitoreo.	23
Figura 10 Identificación del rack primario (alojamiento del Cluster).....	23
Figura 11 RACKS primarios rack 2, rack 3 rack 4 del centro de datos.	24
Figura 12 MDF Rack2/ Rack3 PBX, del centro de datos.	25
Figura 13 Distribución física IDFs en planta (NAVE 1 ENSAMBLES).....	26
Figura 14 Distribución física IDFs en planta (NAVE 2 BREAKERS).	26
Figura 15 Identificación de IDF-1 Vigilancia (Surveillance).	27
Figura 16 Identificación de IDF-2 Embarques (Shipping).	28
Figura 17 Identificación de IDF-3 Recibo (Receiving).	28
Figura 18 Identificación de IDF-4 Pintura (Paint).	29
Figura 19 Identificación de IDF-5 Mantenimiento (Maintenance).....	29
Figura 20 Identificación del IDF-6 QOM2 BRK.	30
Figura 21 Identificación de IDF-7 Mille Auto BRK.....	30
Figura 22 Identificación de IDF-8 Mezzanine BRK.....	31
Figura 23 Identificación del IDF-9 Almacén Breakers (Wharehouse BRK).	31
Figura 24 NetBotz Room Monitor 750.	46
Figura 25 NetBotz Wall Monitor 755.	47
Figura 26 Compatibilidad y aditamentos del NetBotz 750 y 755.....	48
Figura 27 NetBotz Room Monitor 750 y puertos de conexión.....	49
Figura 28 Primer NetBotz 750 (Superior del rack del servidor).	51
Figura 29 Segundo NetBotz 750 (Inferior del rack del servidor).	52
Figura 30 Integración de manijas en racks y sensores de temperatura.	52
Figura 31 Instalación de sensor de humo, manija interna, e interruptor de puerta.	53
Figura 32 Implementación de manijas inteligentes.	53
Figura 33 Cambio del almacenamiento del clúster.....	54
Figura 34 Espacio designado al banco de energía interno del centro de datos (ANTES).	54
Figura 35 Implementación almacén de batería de 8 módulos PX 40KW.....	55
Figura 36 Dispositivos en funcionamiento (cámaras, sensores, y manijas inteligentes).	55
Figura 37 IDF-1 Instalación de NetBotz 755 y UPS Vigilancia (surveillance).	56
Figura 38 IDF-2 Instalación de NetBotz 755 y UPS Embarques (shipping).	57
Figura 39 IDF-3 Instalación de NetBotz 755 y UPS Recibo (receiving).....	57
Figura 40 IDF-4 Instalación de NetBotz 755 Pintura (paint).....	58

Figura 41 IDF-5 Instalación de NetBotz 755 y UPS Mantenimiento (Maintenance).....	58
Figura 42 IDF-7 Integración de cámara inteligente Mille Auto BRK.	59
Figura 43 IDF-6 Instalación de NetBotz 755 QOM2 BRK.	59
Figura 44 IDF-8 Implementación de dispositivos inteligentes Mezzanine BRK.	60
Figura 45 IDF-9 Instalación de NetBotz 755 y rack, Almacén (Warehouse BRK).....	61
Figura 46 Verificación de funcional de banco de baterías del centro de datos.....	62
Figura 47 Verificación funcional del banco de energía en sala (Mezzanine).	63
Figura 48 Verificación funcional de UPS.	64
Figura 49 SE Interfaz NetBotz	65
Figura 50 Verificación funcional del NetBotz 755.	66

Tabla 1. Cuadro comparativo entre metodologías.....	12
Tabla 2. Lista de aditamentos APC requeridos para la implementación.....	42
Tabla 3. Descripción de características y ventajas del dispositivo NetBotz 750 en su implementación.	46
Tabla 4. Descripción de características y ventajas del dispositivo NetBotz 755 en su implementación.	47
Tabla 5. Opciones de configuración de red en el dispositivo.....	50

CONTEXTO GENERAL DEL PROYECTO

Introducción

Schneider Electric Planta Tlaxcala (SE), se encuentra ubicada en carretera vía corta Santa Ana Chiautempan a Puebla km 17.5 en la comunidad de Acuamanala Tlaxcala, específicamente la planta se encarga en destacar la fabricación de producto estándar que incluye: gabinetes metálicos, moldeo, estampado, taller de maquinado, y su producto principal los interruptores termo magnéticos (breakers), es una de las diversas plantas que pertenece a una misma organización y que cuenta con servicios indispensables TI.

El soporte TI interno se ha centrado en los procesos por hacerla más eficiente en todas sus funciones como: administrar, optimizar, configurar y recopilar datos de los servicios físicos TI, y por ende de ellos generar la productividad en el negocio. En toda la planta se toma seriamente la intervención de automatizar los procesos tecnológicos e implementar medidas de seguridad haciendo de este el fortalecimiento del negocio.

Con el crecimiento de la planta y con la llegada de nuevas líneas de producción se demandan más aspectos tecnológicos que son indispensables y que aportan la vitalidad a los demás servicios, esto exige el crecimiento en el área de sistemas y sobre todo una mayor cobertura para remodelar la infraestructura basada en las mejoras de la seguridad. Así mismo se planearon estrategias TI desde altos mandos para que sus contribuyentes tecnológicos pudieran establecer la idea de hacerlo distinto e innovador, donde se realizó un estudio de las demandas y necesidades tecnológicas de la infraestructura interna de la planta.

El planteamiento de una resiliencia es una realidad, y un compromiso en todo tipo de organizaciones, porque ejerce la continuidad del negocio a través de la recuperación de incidentes, por medio de respuestas inmediatas. La resiliencia juega un papel importante para cubrir necesidades deficientes, como son las medidas de seguridad y el control a accesos a los centros de datos, la integración de dispositivos automatizados, como los sistemas de notificación de emergencia, el monitoreo ambiental, y la intervención de sistemas de alimentación ininterrumpida, todo esto basado y limitado a un marco únicamente físico que es el hardware.

La industria no solo ofrece las ventajas de implementar buenas prácticas tecnológicas en la estrategia del negocio, sino también de cumplir con los objetivos que se exigen. Al mismo tiempo, esto centra la misión de la organización, mostrando así una mirada integral donde se tendrá un panorama claro entre los servicios y las tecnologías de la información. De igual manera, se verá reflejado en el desarrollo e implementación de los cambios que se requieren en la infraestructura física tecnológica, basada en cubrir sus necesidades y en el establecimiento de funciones que aseguran la óptima gestión de los servicios de TI.

La organización es pionera para generar respuestas inmediatas, por ende se involucra el uso de dispositivos ups de la línea (APC) ya existentes en el mercado, la importancia de utilizar estos recursos hará de la infraestructura física más resiliente potencializando aún más los servicios tecnológicos ya existentes a través de sus canales físicos que se estudian en este proyecto, los cuales son guiados y dirigidos con una metodología orgánica para moldear los procesos y proveer la protección de los dispositivos principales que generan la comunicación.

Los procesos de resiliencia permiten establecer estrategias claras que se abordan mediante una metodología estructurada, basándose en normas y procedimientos ya existentes. Aunque detrás de estas acciones existe un presupuesto, este no se mencionará en este proyecto por razones legales y políticas de la organización. Sin embargo, se detallarán los aditamentos como herramientas clave que facilitarán los procesos necesarios para que la organización se vuelva más resiliente. El departamento central es responsable de proporcionar los recursos necesarios para que la administración de TI del sitio implemente las mejoras estratégicas, con el objetivo de fortalecer la planta a nivel local.

Planteamiento del problema

En los últimos años la planta se ha visto internamente afectada por agentes externos, tales como personal de estancia corta (visitantes, proveedores) y administrativos externos del área tecnológica. El rubro más visible e importante a cubrir es la seguridad. La falta de automatización y renovación de ciertas áreas de la infraestructura física tecnológica son sumamente un problema notorio y en consecuencia ha generado la ausencia de monitoreo al principal centro de datos de la planta. La identificación de las amenazas y los nuevos ambientes de riesgos a los que se exponen la organización son cuestiones de seguridad, e influye en todos los dispositivos físicos que hacen que se pueda dar la comunicación interna y externa.

Estas son las razones principales que intervienen y generan deficiencia desde una visión general por parte del departamento interno de TI de la planta, siendo éste un tema relevante que engloba a todo un sistema de seguridad, por ello se plantea la implementación de una resiliencia de la infraestructura que permita ayudar a los servicios físicos, a cubrir los criterios de las tecnologías de la información TI.

Cubrir las necesidades faltantes dentro del servicio tecnológico es fundamental para la continuidad del servicio dentro del negocio. A continuación se enlistan:

- Inexistencia de cámaras de vigilancia y monitoreo de accesos a los ingresos del “centro de datos”.
- Falta de control de acceso en las puertas de los racks del principal centro de datos.
- Ausencia de monitoreo y control de temperatura al hardware de procesamiento de datos (IDFs).
- Ausencia de UPS para equipos críticos de producción que se manejan sobre líneas intermediarias, IDFs y data center.

Estas son las principales razones que afectan la seguridad en los procesos internos de la planta, el simple hecho de no llevar un control de monitoreo en los accesos genera que se vea afectado todo un control de restricciones que generalmente ocasiona robo, extravío, y accesos no autorizados a áreas restringidas de gran valor de información digital, paralelamente se identificó que hay sobrecalentamiento en los equipos provocando pérdida de rendimiento, en conjunto con el corte de suministro de energía por falta de dispositivos UPS, esto ha generado fallas críticas a equipos ocasionadas por apagones, que esporádicamente causan paros en líneas de producción, por lo que es necesario incidir en una resiliencia como una estrategia de aspecto fundamental, que claramente exige mejorar la calidad en los procesos internos para la productividad de la planta.

Justificación

El presente proyecto se enfocará en la implementación de una resiliencia basada en el uso de dispositivos tecnológicos que le permitirán a la planta enfrentarse de forma exitosa a cambios de eventos internos como externos, permitiendo así minimizar los riesgos u amenazas de la infraestructura en la planta, ya que la falta de automatización física ha ocasionado un conflicto en la seguridad de los recursos internos de los sistemas de comunicación en Schneider Electric Tlaxcala. Hoy en día es indispensable contar con servicios tecnológicos resilientes que sean capaces de ser persistentes y funcionales ante las circunstancias de adversidad, logrando así el enfoque que marca la resiliencia en la continuidad del negocio, y cubriendo el rubro de requerimientos del hardware. Este trabajo permitirá mostrar que la resiliencia tecnológica en el hardware es una estrategia clave que ayuda a la industria a establecer sistemas sólidos, y por ende mejora las habilidades tecnológicas a través de la diversificación contribuyendo a los mecanismos de seguridad.

Objetivos

General

Establecer la implementación de una resiliencia para la infraestructura física TI como una estrategia de conservación a la confiabilidad de los procesos del servicio, ante la planificación, la implementación y la contribución de soporte y mantenimiento, basada en cubrir los criterios de seguridad y automatización de la infraestructura TI, cuyo enfoque se basa en promover la eficacia de los componentes y la administración de los servicios tecnológicos físicos a nivel local.

Específicos

1. Implementar la metodología Ágil (Scrum) para gestionar eficientemente la instalación de hardware y mejoras en la infraestructura tecnológica.
2. Aplicar marcos y estándares de seguridad que fortalezcan la continuidad del negocio y la resiliencia en la gestión de servicios de TI.
3. Realizar un diagnóstico de los componentes físicos en deterioro para planificar su corrección o reemplazo y garantizar la seguridad en el centro de datos.
4. Instalar sistemas de monitoreo y control de acceso en el centro de datos para prevenir riesgos y mejorar la seguridad de la infraestructura.
5. Analizar el impacto de la resiliencia en la infraestructura de TI para optimizar la eficiencia operativa y mitigar riesgos.

Alcances

El estudio explora la resiliencia como el fundamento hacia la mejora a los procesos de prevención, recuperación y adaptación de las circunstancias donde puedan surgir eventos que contribuyan al “riesgo”, con lo cual la resiliencia es fundamental para definir a la infraestructura TI como una propuesta dirigida al cambio para la salud de los servicios físicos que emplean la comunicación.

El estudio del sitio abarca la mejora del equipamiento físico, como: el monitoreo ambiental, dispositivos de seguridad, tarjetas de proximidad, control de acceso, enfriamiento, sensores de humedad, sensores de temperatura, grabación ininterrumpida, y el control de suministro eléctrico a partir de sistemas de alimentación (UPS).

Implementar los sistemas de seguridad y monitoreo, donde se pretende mejorar y reforzar aspectos tecnológicos, y al mismo tiempo lograr automatizar estos.

Limitaciones

1. La resiliencia de infraestructura TI va dirigida solo aquellas plantas a nivel Norteamérica y Latinoamérica que su infraestructura requiera de necesidades tecnológicas, esto para el cumplimiento de los criterios de las normativas tecnológicas industriales, pero el estudio e implementación de servicios se limita únicamente para la matriz de la planta local, no para la organización general.
2. Dentro de los limitantes del presente trabajo no abarca la etapa de la gestión de recursos, como: la obtención de insumos. Así como temas de presupuestos por cuestiones políticas de la organización, se prohíbe exhibir información detallada por parte del departamento de TI.
3. La investigación no se extenderá en áreas fuera de la cobertura del negocio a implementar, únicamente en la instalación técnica superficial llevando a cabo así la adaptación de esta a la infraestructura, y no tratase de generar ningún manual de los dispositivos técnicos utilizados.
4. Solo se hace mención de la comunicación lógica a nivel técnico superficial de los equipos que son instalados. Por ende, no serán expuestas direcciones IP de los dispositivos conectados, de igual manera no se cuenta con las credenciales como el control de accesos de configuraciones de red, así como contraseñas de administrador para acceder al software de los diferentes dispositivos conectados, ya que el Departamento de Consultores TI Conectividad (redes), se encarga de la gestión para crear los enlaces de comunicación para su operación lógica, todo ello como limitantes para preservar resguardo de información dentro del departamento interno TI.

5. La colaboración con terceras personas (proveedores, consultores IT (redes)) es para cubrir ciertos requerimientos y necesidades que son parte de la gestión e involucramiento administrativo, y solo son mencionados para hacer referencia a los procesos que se intervinieron para la factibilidad del proyecto.
6. El proyecto no se centra en la profundidad de los riesgos, se consideran y se hablan de estos de forma relativa, pero sin enfocarse en los eventos de riesgo de alto impacto, así como en la mención de normativas.
7. La información obtenida y redactada es la proporcionada por la empresa a la fecha de inicio del proyecto, y sus alcances están en base a la misma, cualquier cambio que se dé al tiempo puede modificar futuras implementaciones.

FUNDAMENTOS TEÓRICOS

Marco Teórico

Janco Associates Inc. (2017) indicó: *“La resiliencia tecnológica se define como la capacidad de una organización para mantener niveles de servicio aceptables a través y más allá de las interrupciones graves de sus procesos críticos y los sistemas de TI que los respaldan.”*

La resiliencia también es conocida en el medio como resiliencia digital o simplemente resiliencia tecnológica, es un conjunto de prácticas operativas que permiten a las organizaciones brindar niveles de servicio óptimos a pesar de las interrupciones en la disponibilidad de la infraestructura de TI. En otras palabras, significa garantizar que sus flujos de trabajo de TI puedan resistir fallas del sistema sin experimentar interrupciones, tiempos de inactividad o pérdida de datos. Con base en el estudio de la resiliencia y su impacto en las tecnologías de la información y comunicaciones se rige bajo una amplia gama de criterios a cubrir, aunque el proyecto esté totalmente delimitado a la seguridad resiliente del hardware. La resiliencia va más allá de cubrir las necesidades del hardware es una gran rama que comprende temas como ciberseguridad que engloba la protección de la red, los datos de los sistemas, la función del software, y de todo un tema de grandes rubros que comprometen componentes de la funcionalidad de un sistema informático.

Así mismo Fireshmit (2019) en esta misma línea, aduce: *“La resiliencia del sistema ha sido ampliamente discutida como una preocupación crítica, especialmente en términos de centros de datos y computación en la nube. También es de vital importancia para los sistemas ciberfísicos.”*

Para comprender este tema, del porque la utilización de una resiliencia, es importante entender de manera redundante la palabra resiliencia:

Según American Psychological Association (2011) *“La resiliencia es el proceso de adaptarse bien a la adversidad, a un trauma, tragedia, amenaza, o fuentes de tensión significativas, como problemas familiares o de relaciones personales, problemas serios de salud o situaciones estresantes del trabajo o financieras. Significa “rebotar” de una experiencia difícil, como si uno fuera una bola o un resorte”*

En pocas palabras la psicología define la resiliencia como la capacidad del ser humano para sobreponerse a las adversidades que se presentan en la vida. Esta habilidad nos permite mantenernos firmes y perseverar, incluso después de enfrentar problemas o situaciones difíciles.

Se comprende que en los sistemas de tecnologías se basan en la misma forma, puesto a que se busca que una organización tenga la capacidad de mejorar sus aspectos de infraestructura o de un sistema, para soportar y recuperarse ante posibles riesgos, o como tal tomando en consideración eventos de desastres, con el fin de proveer, y mantener en forma aceptable sus operaciones y servicios, ya sean físicos, o lógicos, de esta forma se propaga un aspecto a medir tan importante como lo es la disponibilidad, para finalmente lograr el poder anticiparse, resistir, recuperarse y evolucionar ante

futuros riesgos u amenazas. Entrando dentro del contexto y teniendo en claro lo que quiere decir resiliencia, ahora es importante saber cómo funciona la resiliencia y qué aspectos se cubren de ella en este trabajo. La resiliencia en la infraestructura TI solo es inicio que puede evolucionar en un corto o mediano plazo a un DRP.

Lefort, A. (2019) indicó: “*Un DRP (Disaster Recovery Plan) o Plan de Recuperación de Desastres, es un sistema con el cual las organizaciones se preparan contra posibles desastres de diversas índoles que pueden dañar la infraestructura tecnológica y por ende poner en riesgo el negocio y finalmente fin a sus actividades operativas.*”

Básicamente un DRP es la toma de toda una estrategia de acciones basados en seguimientos sumamente precisos, y de restablecimientos de servicios de TI ante cualquier eventualidad, pero con un enfoque más profundo que la resiliencia, logrando precisiones exactas de la estabilidad de un evento más crítico en tiempos sumamente cortos y sin pérdida de información englobando todos los aspectos de los servicios tecnológicos. Esto no solo cubre la infraestructura tecnológica, sino más aspectos que también involucran subáreas que no necesariamente pertenecen a las TI. En lo particular la planta en mención, aún no cubre en su totalidad los requerimientos de un DRP pero se pretende que sea la evolución de la resiliencia, por ello la importancia de este proyecto, puesto que puede ser una acción importante, que por ende generara un gran impacto.

El propósito de una resiliencia en la industria.

Según un informe de la Southern New Hampshire University, el 62% de los responsables de seguridad informática en empresas informan sentirse poco seguros o nada seguros con respecto a los sistemas informáticos en sus organizaciones. En contraste, solo el 7% se siente muy seguro en esta área.

Con base en la información, es sumamente importante para la planta tener un respaldo a nivel lógico y físico, considerando el enfocado en su parte física, se puede ver el requerimiento de nuevas alternativas, la empresa ya cuenta con ciertos dispositivos que claramente hacen su función, pero es necesario tener nuevas estrategias como dispositivos que prolonguen vida útil y al mismo tiempo automaticen la seguridad infraestructural, simplemente porque garantizan y aseguran la continuidad de las operaciones comerciales con total transparencia para los usuarios y administradores.

Aquí entra un punto sumamente importante que es la integración de los servicios tecnológicos, estos se refieren a aquellos que emplean la tecnología para respaldar, optimizar o gestionar diversas operaciones dentro de una organización o para sus usuarios. Estos servicios abarcan una amplia gama de funciones, y su principal propósito es asegurar que las herramientas tecnológicas funcionen de manera eficiente y segura.

Algunos ejemplos de estos servicios son:

1. Administración de redes y conectividad: Se garantiza que los dispositivos y sistemas estén adecuadamente interconectados, asegurando así un funcionamiento seguro y eficiente de las redes.
2. Soporte técnico: Es proveer de apoyo técnico para abordar problemas relacionados con hardware, software o redes.
3. Ciberseguridad: Son servicios destinados a resguardar sistemas, redes y datos frente amenazas como los virus, ataques cibernéticos o filtraciones de información.
4. Almacenamiento y administración de datos: Dar y proporcionar soluciones para almacenar, estructurar y gestionar información, ya sea en servidores locales o en plataformas de almacenamiento en la nube.
5. Instalación de hardware y software: Se hace la instalación, configuración y mantenimiento de equipos físicos, como computadoras, servidores, etc. así como de los programas informáticos para el correcto funcionamiento de eficaz dentro de la empresa.
6. Supervisión y cuidado de los sistemas: Control continuo de las tecnologías y sistemas para garantizar su funcionamiento adecuado y detectar problemas antes de que impacten el rendimiento.
7. Soluciones en la nube: Proporcionan almacenamiento, procesamiento y acceso a aplicaciones y datos mediante internet.
8. La automatización de procesos: Es la parte innovadora de los sistemas y consiste incorporar tecnologías como la robótica y sistemas inteligentes para llevar a cabo de manera automática tareas repetitivas o manuales.

A partir de estos aspectos mencionados, se busca garantizar que los sistemas estén bien distribuidos en relación con los dispositivos físicos y que estén sincronizados mediante un equipamiento que gestione adecuadamente la infraestructura. Esto permitirá que continúen funcionando de manera efectiva incluso después de una conmutación.

En otro contexto de igual forma se puede considerar que la resiliencia operativa adquiere relevancia debido al ambiente que se genera alrededor de las organizaciones por las necesidades cambiantes, basados en términos de riesgos y oportunidades. El objetivo es claro, y es tener una organización que cuando sufra una disrupción repentina, tenga la capacidad recuperar sus operaciones, todo esto involucrando a la protección de la infraestructura, por lo cual relaciona la información contenida y circulante, es por ello que existen herramientas tecnológicas concebidas para minimizar los posibles riesgos, siempre con el fin de contribuir a la gestión de la seguridad del negocio.

Específicamente reafirmando ya lo descrito desde el comienzo, la resiliencia es sencillamente la capacidad de una empresa para resistir y recuperarse de perturbaciones ante crisis o eventos adversos, y esto es también conocida como resiliencia en la industria. El objetivo principal la resiliencia industrial abarca aspectos como la continuidad del negocio, la protección de activos críticos, la gestión de crisis, y sobre todo la capacidad de adaptación y flexibilidad, refiere mayormente en mantener las operaciones comerciales funcionando para minimizar el impacto en sus activos, empleados, clientes y en su reputación. La resiliencia en el ámbito industrial implica la capacidad de ajustarse y adaptarse a cambios en el entorno de operaciones, ya sea por razones internas como modificaciones en la estrategia empresarial o externas como variaciones en el mercado o desastres naturales. Las organizaciones resilientes son flexibles y pueden actuar rápidamente para hacer frente a nuevos desafíos.

En general la resiliencia industrial contribuye a proteger la reputación en todo el contexto del negocio y sobre todo preservar la confianza de una empresa ante clientes, socios comerciales, inversionistas y otras partes interesadas. Es una respuesta eficaz ante crisis y situaciones adversas puede ayudar a mantener la confianza del público y reducir al mínimo el impacto negativo en la imagen corporativa. El objetivo de fomentar la resiliencia en el sector industrial es asegurar la supervivencia y prosperidad a largo plazo de las organizaciones, fortaleciendo su capacidad para resistir, adaptarse y recuperarse ante desafíos y perturbaciones en un entorno empresarial cada vez más complejo, variable y sobretodo competitivo.

MÉTODO ESTRATÉGICO PARA LA IMPLEMENTACIÓN DEL PROYECTO

Metodología

Para la elección de la metodología se utilizó una revisión de documentos, la cual facilitó la exploración, la comprensión, y el estudio de los datos necesarios para la investigación. En el entorno del desarrollo del software se encuentran diversas gamas de metodologías que comparten similitud en ciertas características y cuyos aspectos se asemejan a otras metodologías, no obstante, no todas se adaptan a los proyectos puesto que su viabilidad para el éxito se debe a diversos factores y requerimientos. Las metodologías que abordan y acompañan a los procesos de construcción de un proyecto de desarrollo de software son posibles de adaptarse a la instalación del hardware, porque comprenden de algo tan sencillo llamado “*gestión*” que abarca una planificación iterativa, la ejecución de tareas, y hasta un control de actividades, estos procedimientos pueden ser aplicados para coordinar actividades al momento de instalar componentes físicos en un espacio en específico, buscando así la adaptabilidad y la capacidad de respuesta al cambio, lo cual cubre al mismo tiempo un punto importante dentro de la resiliencia TI operacional. Prácticamente las técnicas de desarrollo de software ofrecen una serie de enfoques y normas que se pueden ajustar e implementar de manera eficaz en la configuración del hardware para asegurar una instalación exitosa y satisfactoria del sistema físico.

En el mismo contexto metodológico que ocupa la ingeniería en software se pretende proyectar esas mismas gestiones para este proyecto, considerando la recopilación de información para ser adaptado y descrito de forma íntegra y de fácil comprensión de los temas que serán abordados, exponiendo así la perspectiva de la resiliencia.

No obstante, ante lo ya comprendido, el estudio de las metodologías es limitado entre la metodología ágil (scrum) y la espiral para la elección adaptativa de este proyecto. Ambas metodologías proveen de un mismo contexto similar al esquema en práctica de la gestión, ya que las dos opciones están diseñadas para abordar herramientas de software que son altamente adaptables a otros proyectos de distintas índoles, en estas metodologías también existen diferencias significativas. La metodología en espiral se enfoca en la gestión de riesgos y se emplea mayormente en proyectos grandes y complejos. En cambio, la metodología ágil está claro que es comúnmente utilizada en proyectos de desarrollo de software, pero tiene el potencial de ser más flexible y es adaptable a otro tipo de proyectos. Además, la metodología en espiral sigue un enfoque formal y es sumamente estructurado, a diferencia de la metodología ágil que fomenta la auto organización y la toma de decisiones por parte del equipo, aun compartiendo enfoques que permiten incorporar cambios de manera eficiente, sin comprometer la continuidad del negocio.

Durante el proyecto se pueden minimizar problemas de compatibilidad, errores de configuración o retrasos en la entrega de componentes, y finalmente la fomentación estrecha de colaboración entre los diversos equipos que participan en el proyecto.

En la Tabla 1 se presentan las metodologías que son aplicables al desarrollo de la instalación de dispositivos como el hardware, para la implementación en la infraestructura TI.

Tabla 1. Cuadro comparativo entre metodologías.

Metodología Ágil(scrum)	Características Distintivas	Metodología en espiral
Desarrollo evolutivo y creciente.	Enfoque	Desarrollo evolutivo y creciente.
Ofrece ciclos cortos.	Procesos de desarrollo	Ciclos largos y subdivididos.
Muy adaptable y versátil frente a cambios.	Adaptabilidad	Flexible con moderación.
Preponderancia en la comunicación, (cara a cara).	Comunicación	Comunicación solo formalizada mediante escritos.
Adaptabilidad continúa a cambios en los requisitos.	Gestión de modificaciones	Variación permitida en momentos concretos.
Rápida identificación y gestión de riesgos.	Posibilidad de riesgo y manejo de control	Detección y control de riesgos en cada fase.
Enfoque más dirigido ante la implementación que en el desarrollo de documentación (reportes breves de las acciones realizadas).	Registro	Elaboración exhaustiva de documentación en cada etapa de implementación
Suministro de características beneficiosas para el sitio tratado.	Aportación de valor	Liberación escalonada de los componentes.

Iteraciones rápidas y frecuentes (en caso requerido).	Iteraciones	Iteraciones menos habituales, pero más completas.

En el contexto que aborda la Tabla 1, otorga el derecho a la pregunta ¿por qué adaptar la metodología ágil en un proyecto como este? La respuesta es simple, la elección de implementarla en este proyecto es porque es más factible cumplir con los criterios que sugiere la metodología, por ende, es adaptativa en la instalación de hardware y puede contribuir a potenciar la flexibilidad, la calidad, la interacción entre el equipo y la eficacia del procedimiento.

De acuerdo con, LATAM (2023) definió “*Una metodología ágil es una innovadora forma de trabajar y organizar flujos, que divide los proyectos en partes, permite adaptarse sobre la marcha, complementa y resuelve etapas en poco tiempo.*”

Concretamente la metodología ágil no se centra en una lista de instrucciones específicas sobre qué hacer durante el proceso de cada proyecto. En cambio, se centra en una mentalidad colaborativa y en la gestión de procesos, estableciendo un conjunto de valores que orientan las acciones y la forma en que se llevan a cabo.

ANÁLISIS Y DESARROLLO

Plan de acciones para establecer la resiliencia

En la planta, se organizan reuniones con el equipo de trabajo de TI para abordar las deficiencias en la infraestructura a nivel local. Estas reuniones permiten identificar problemas evidentes, como la falta de renovación del cableado estructural dentro de los IDF (Intermediate Distribution Frame). Entre otros aspectos más, A partir de estas observaciones, se pueden implementar soluciones de automatización que mejoren la seguridad y faciliten el monitoreo del estado actual de la infraestructura.

Durante las reuniones semanales, se identificaron aspectos indispensables para impulsar el crecimiento del proyecto. Considerando las políticas de calidad exigidas en la industria, se estableció un marco que guiará la implementación del proyecto en su totalidad, es fundamental comprender los criterios necesarios para establecer una resiliencia efectiva, más allá de los ajustes tecnológicos, existe una fase administrativa que permite a los expertos de TI integrarse no solo en el aspecto técnico, sino también en los procesos de respuesta y de formación como gestores administrativos. Estos aspectos se representan en la (Figura 1) como enfoques de cumplimiento.

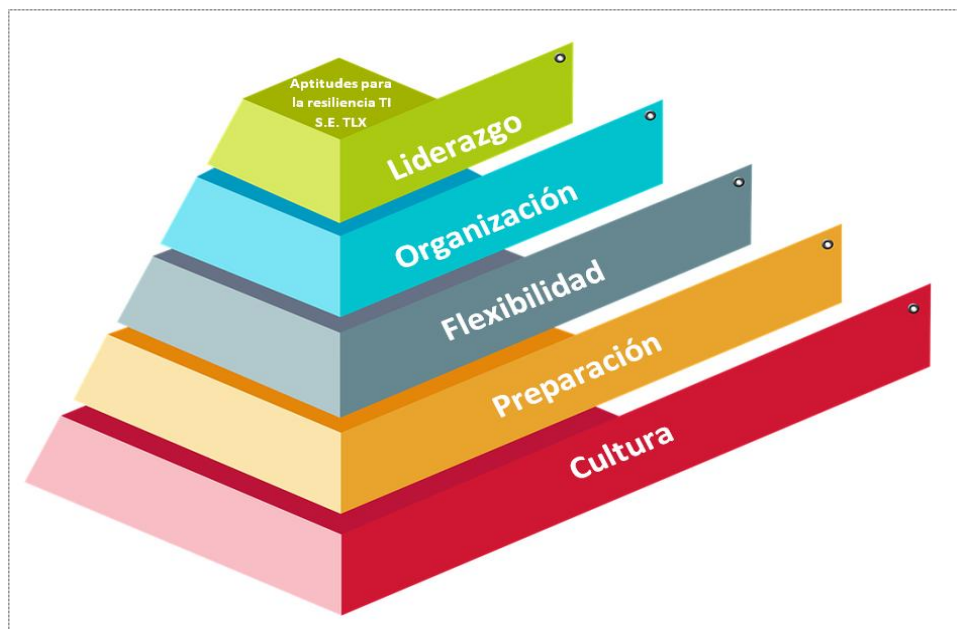


Figura 1 Factores para lograr la resiliencia organizacional.

Liderazgo

Este elemento se considera sumamente importante en la resiliencia organizacional, porque el liderazgo es una habilidad importante en un socio tecnológico dentro de la organización, este factor trata de establecer prioridades, y hacer compromisos ante las capacidades de tomar las decisiones correctas sobre las acciones a tomar cuando se requiera la asistencia para resolver situaciones.

La disciplinaria de ser organizado

El ser organizado es llevar los esquemas en práctica dentro de la industria, se aprende de los procesos para implementar la gestión del trabajo interno, esto quiere decir que no es solamente el tomar las responsabilidades, más bien es hacer el cambio en busca de dar la mayor atención y ofrecer una buena solución, es lograr identificar las interrupciones por adelantado, tomar la recopilación de datos y de proporcionarle a la gerencia el estado actual de las cosas.

La flexibilidad

Este proyecto permite que los recursos de la planta puedan adaptarse a nuevas circunstancias para potencializar los activos físicos, la resiliencia accede a través de un equipo de TI para ser gestionada e implantada. La flexibilidad también se logra mediante la creación de redundancia o copia de seguridad en los sistemas, de tal forma esto le permite a un equipo personas la distribución de actividades.

Preparación y planificación

Como ya se mencionó en la flexibilidad la planta esta activamente anticipada a los problemas y prepararse para ello en comunión con el trabajo en equipo, y sirve como lluvia de ideas ante la planificación de emergencias que ejerzan soluciones como el actuar con eficacia y reducir “riesgos”, estos ejercicios preparan al equipo para mantener activamente a la planta y así hacer frente a los problemas.

La resiliencia a través de una cultura

La confianza y la responsabilidad implica un sentido de propósito compartido, es fomentar hacia una cultura más consciente del entorno, apoyando la comunicación a través de los planos de trabajo que se puedan ir suscitando, creando una cultura de apoyo organizacional es la clave para el manejo y la gestión de crisis, siendo así un medio a la cultura de la organización para mantener siempre la flexibilidad ante el uso de herramientas e indicaciones que coordinan los trabajos para determinadas acciones.

A partir de la comprensión de la Figura 1 actualmente le permite a la organización poder cumplir con su propósito y conducir hacia un objetivo, cada factor se promueve con base al desarrollo y potencialización de este tipo de proyectos promoviendo la continuidad del negocio del que se mencionara más adelante, considerando en conjunto los aspectos que involucran la gestión (Véase Figura 2).

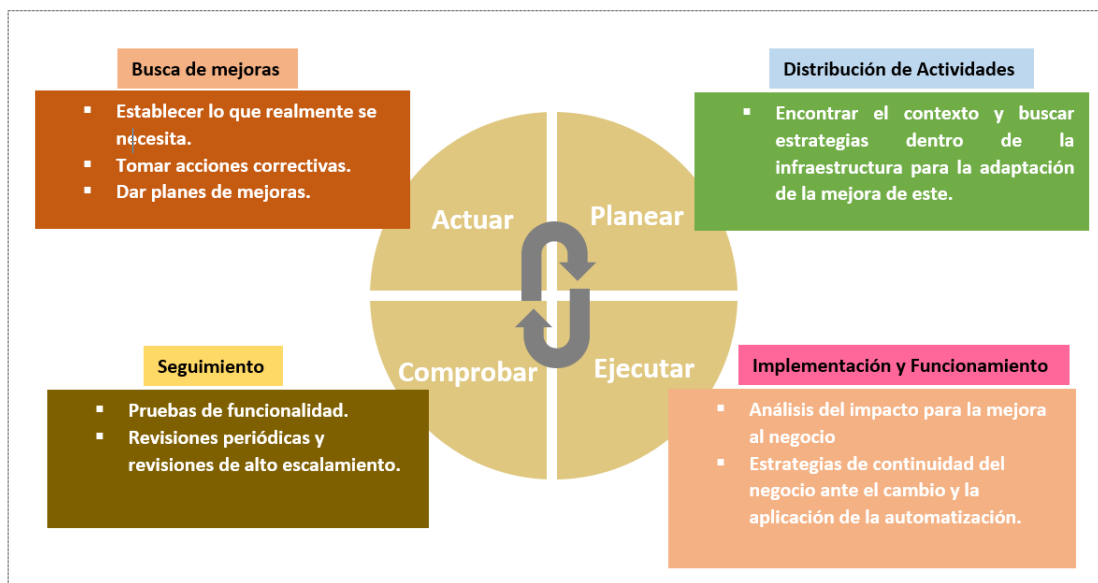


Figura 2 Aspectos de gestión para la continuidad del proceso de resiliencia.

El proceso organizativo propone criterios que cumplan con los requerimientos y ayuden a ampliar el panorama de las necesidades, tales como: ¿Qué se requiere para mejorar la infraestructura interna?, ¿Qué aspectos se deben considerar en el cambio?, ¿Qué se debe lograr?, entre otros. En cada reunión se tomaron decisiones que llevaron a ejecutar acciones decisivas para definir un plan de trabajo y, de este modo, organizar las estrategias que cubran las necesidades de la planta.

A partir de esas estrategias que conforman la continuidad del proceso de la resiliencia se prevén las necesidades que son totalmente funcionales. Todo enfocado a la parte del cambio y de lo que se desea implementar.

Todos y cada uno de estos aspectos son convertidos a producto de la gestión administrativa de las necesidades que se requieren internamente en la planta, es sumamente sencillo ver y considerar esos aspectos deficientes porque eso genera tomar acciones al respecto. La administración interna de tecnología de la planta implica colaborar con proveedores de servicios con el objetivo de acrecentar a la empresa y ello establecer un socio estratégico para cualquier iniciativa que permita ofrecer nuevos servicios a partir de las necesidades que surjan dentro del proceso.

El plan de actividades (Véase Figura 3) se inició basado en un cronograma, en el cual se describe de manera general y simplificada, la inspección del sitio, la construcción de requerimientos a ocupar, la requisición de compra, la finalización de adquisiciones entrantes, mientras que al mismo tiempo se va generando la parte de la implementación de cada uno de los dispositivos a ocupar, y por último la prueba final, y la recepción de información adicional por parte directiva.

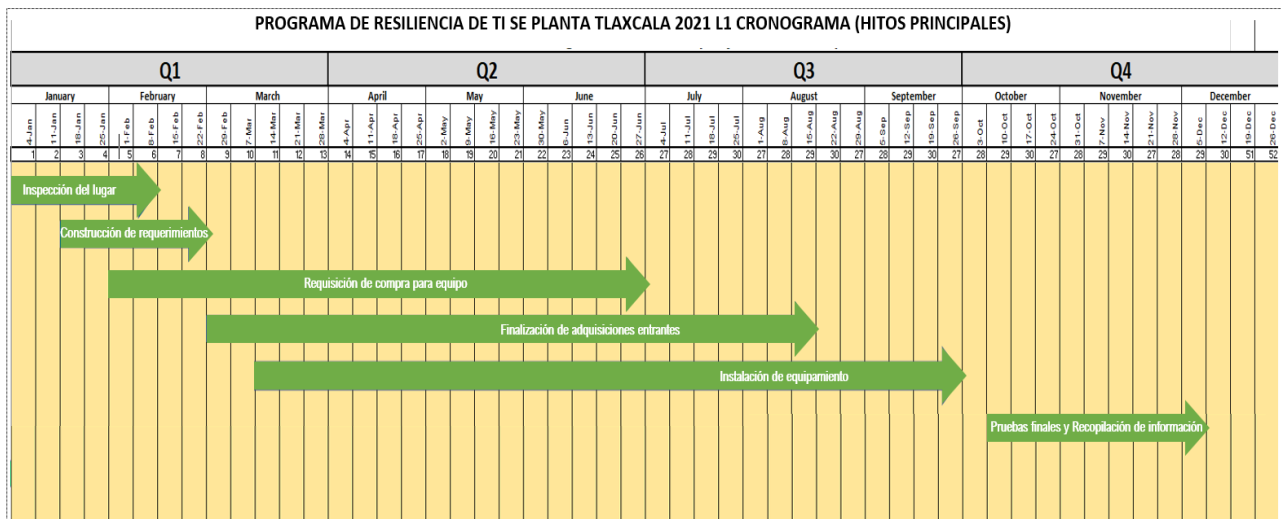


Figura 3 Cronograma de actividades.

Cada una de estas actividades es sumamente importante porque enmarca requisitos importantes que se abordan en la inspección del sitio. En la Figura 4 se describe minuciosamente las acciones que se requieren para fortalecer el proyecto.

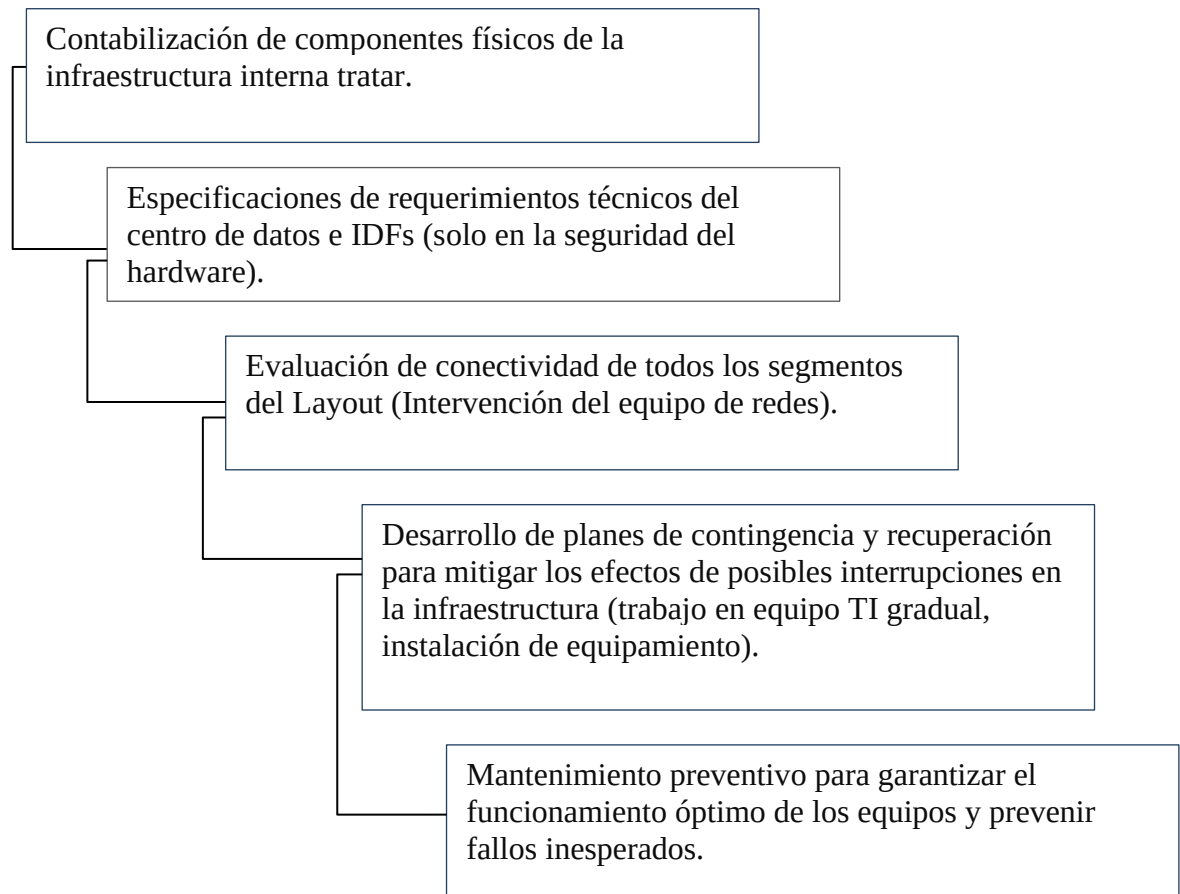


Figura 4 Requerimientos de la infraestructura física interna.

En todo este proceso se incluye la mayor parte los requerimientos de energía y refrigeración como: UPS/alimentación que integran al interruptor de transferencia automática, monitoreo ambiental (sensores), piezas de repuesto, red/conectividad, control de acceso, etc. Aspectos generales que se irán involucrando en el proceso de la implementación.

Identificación de la infraestructura física interna y descripción general de requerimientos

En una identificación de la infraestructura física interna y sus requerimientos, es importante seguir un proceso sistemático. En ello se engloban las estrategias, y con esto se pretende enfocar las necesidades internas como el centro de datos, la revisión de la distribución de los recintos de comunicación secundaria (IDF) que se encuentran internamente y se representa en la Figura 5.

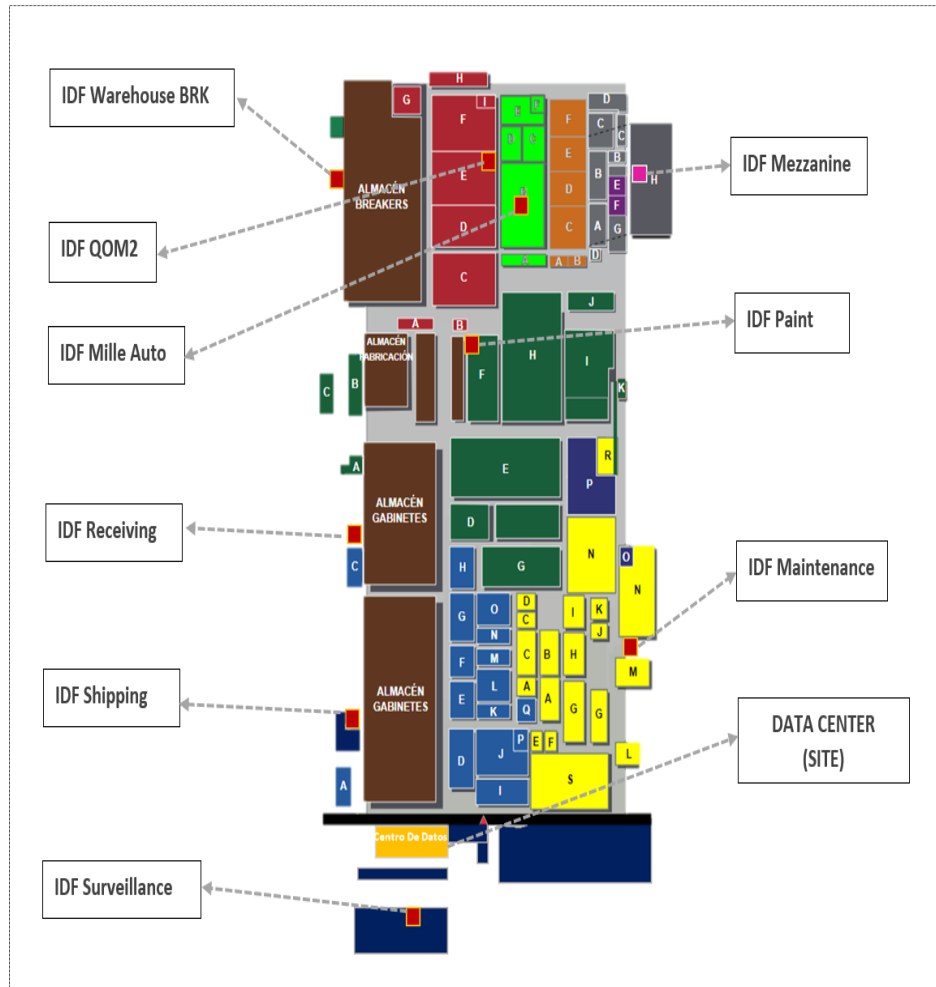
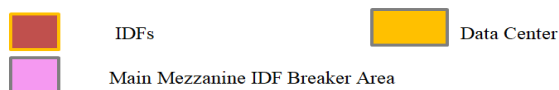


Figura 5 Layout (Diseño interno, y distribución visual de la planta).



Tomando en cuenta el esquema de la infraestructura Figura 5 de la planta se comprende la distribución de los equipos en comunicación, lo cual permite detectar los dispositivos que son considerados para el proceso de integración resiliente, los cuales se distribuyen dentro de los dos segmentos (naves) de la planta.

En la Figura 6 se muestra las cuatro necesidades de los servicios de comunicación, dispositivos complementarios que son considerados para abarcar el proyecto, y que son sumamente redituables para dar los primeros cimientos resilientes. Cada una de estas partes será identificada y enlazada entre sí para mostrar cómo todos estos sistemas se integran en la infraestructura tecnológica de la organización.

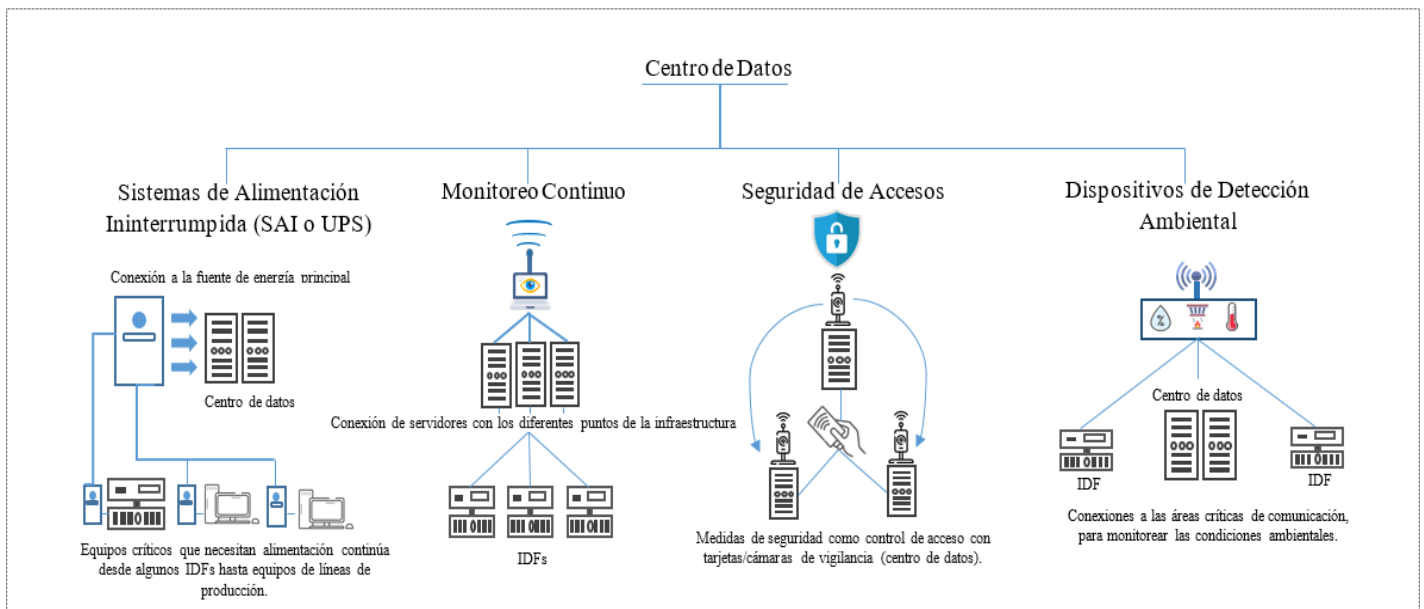


Figura 6 implementaciones para los sistemas de comunicación.

Dentro del análisis no se estableció como tal un lugar concreto de inicio, pero el enfoque personal propio, es enfatizar segmentos de inicios congruentes, por ende, se consideró establecer el arranque de inspección del sitio del “centro de datos” mejor conocido internamente como (site), siendo éste el cerebro operativo de toda comunicación interna y externa que abarca todos los rubros del negocio.

A continuación, se muestra la Figura 7, que representa el estado preliminar del centro de datos antes de la implementación de las medidas de resiliencia en la infraestructura.



Figura 7 Principal Centro de Datos de SE Planta Tlaxcala.

La distribución interna se encuentra asociada ya con elementos que generan funcionalidad como; una unidad crac, un panel de energía UPS de 40 kva. Con estos elementos se sostiene en marcha del estado de ventilación y respaldo energético como necesidades básicas de una sala para el continuo funcionamiento de los servicios, así como se muestra en la Figura 8 se identifican los bastidores con más relevancia, todo esto basado a las necesidades primordiales y a los ciertos tipos de criterio que son considerados para la manipulación y renovación tan solo en los racks, únicamente se consideran los que pertenezcan de la línea APC para implementarles modificaciones, donde más adelante se mencionará más sobre este tema. Cabe aclarar que solo ciertos bastidores no entran en esa línea de mejora de la seguridad en cuanto las puertas y manijas, en este caso se descartan de una implementación de mejora según el lineamiento que indica la gerencia del departamento TI.



Figura 8 Racks internos del Centro de Datos.

Se observa la parte interna del centro de datos de la Figura 8, como cada uno de los racks alojan los servicios como: el servidor, la fibra óptica, PBX, MDF etc. En la imagen izquierda se muestra un espacio marcado el rojo de medidas de 60x60 cm se planteó ser considerado para tener un segundo banco de baterías.

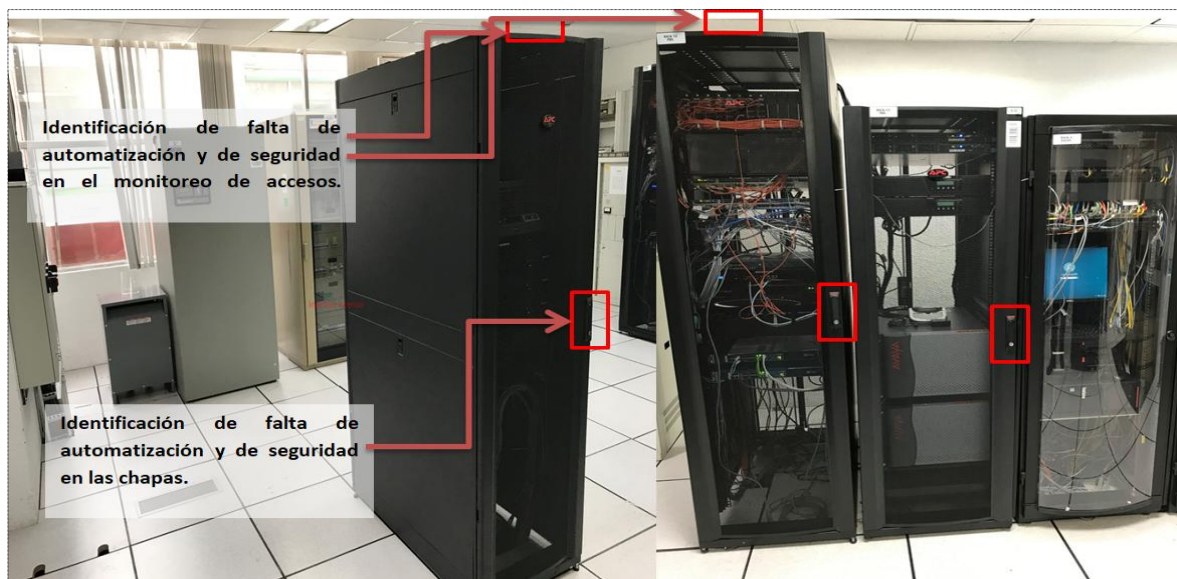


Figura 9 RACKS del centro de datos con deficiencia de seguridad en chapas y monitoreo.

A simple vista se considera ya la búsqueda de automatizar una parte en los gabinetes (Racks), como los que se muestran Figura 9 -10 como ya se mencionó solo abarcan gabinetes con especificaciones de la línea APC puesto a que son viables para implementar automatización en las chapas de las puertas de los gabinetes para la mejoría y control en el acceso.

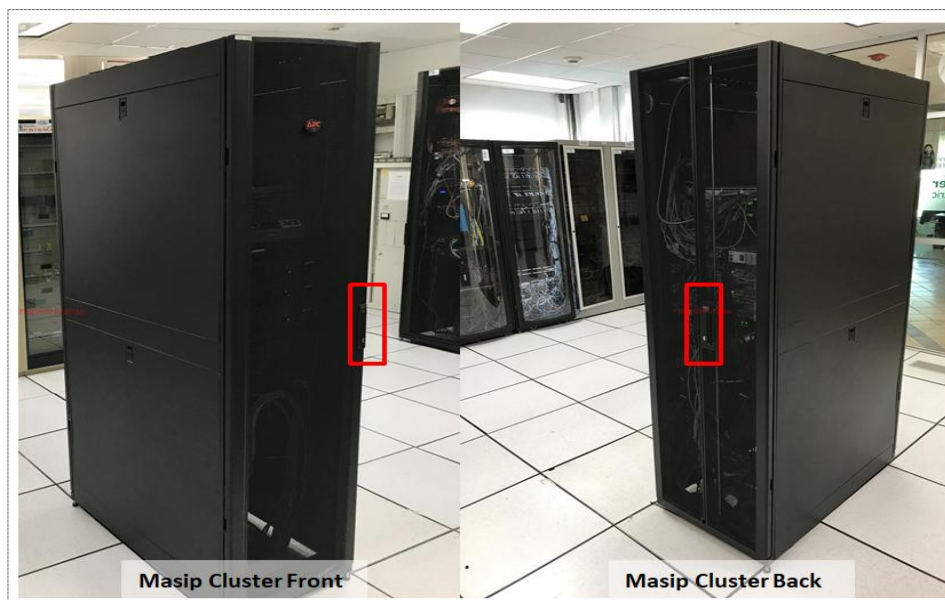


Figura 10 Identificación del rack primario (alojamiento del Cluster).

En la Figura 10 se muestra el rack que contiene el servidor usualmente se abre más por cuestiones de montaje de cambio de cintas, y se puede observar que hay manijas manuales en la parte frontal y trasera del rack, usualmente son fáciles de abrir sin ningún inconveniente y eso genera inseguridad, por lo cual puede generar una mala manipulación de este. Las puertas y chapas de este tipo de rack deben ser más sofisticados, cumpliendo así con el requerimiento para poder ser automatizados. De igual modo en la Figura 11 se observan las consideraciones que se le pueden anexar a esos racks primarios.



Figura 11 RACKS primarios rack 2, rack 3 rack 4 del centro de datos.

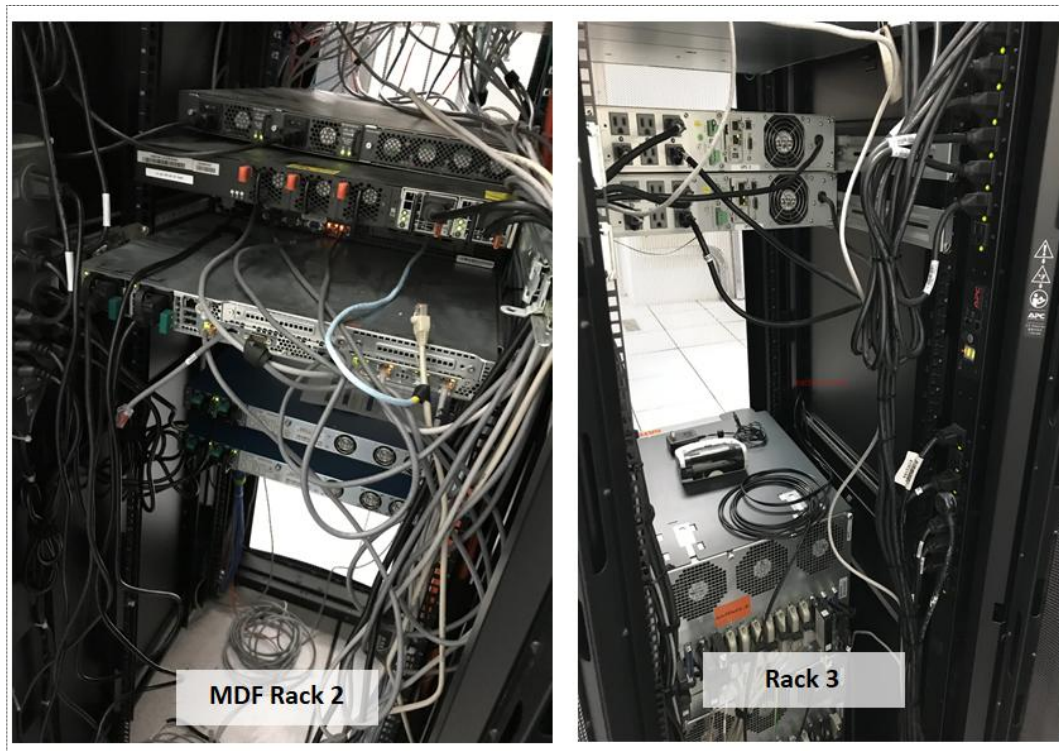


Figura 12 MDF Rack2/ Rack3 PBX, del centro de datos.

En el medio de identificación de estos procesos esta la Figura 12, visualiza el MDF principal del servicio de distribución de red, el PBX (red de telefonía privada) y el rack de servicio de datos. Aunque solo por esta vez únicamente ingresa como principales objetivos la manipulación de automatización en puertas y manijas en los rack 1, 2, y 3 ya que son sumamente esenciales para la implementación de otros dispositivos que más adelante se especificarán.

Identificación de IDFs en planta

Basado en el diseño layout Figura 5, se encuentra toda la conexión que se genera del centro de datos a los IDFs, prácticamente funcionan como la distribución intermediaria de todas las comunicaciones en planta.

El fin representativo, es ver la parte esencial de monitorear cada uno de estos racks que finalmente distribuyen información que viaja por medio de cables, y fibra óptica, que a su vez están interconectados en interruptores. Se presentan a continuación en las Figuras 13-14 se comprende la arquitectura funcional basada en la distribución de la comunicación que se encuentra dentro de las dos naves de operación que hay internamente en la planta.

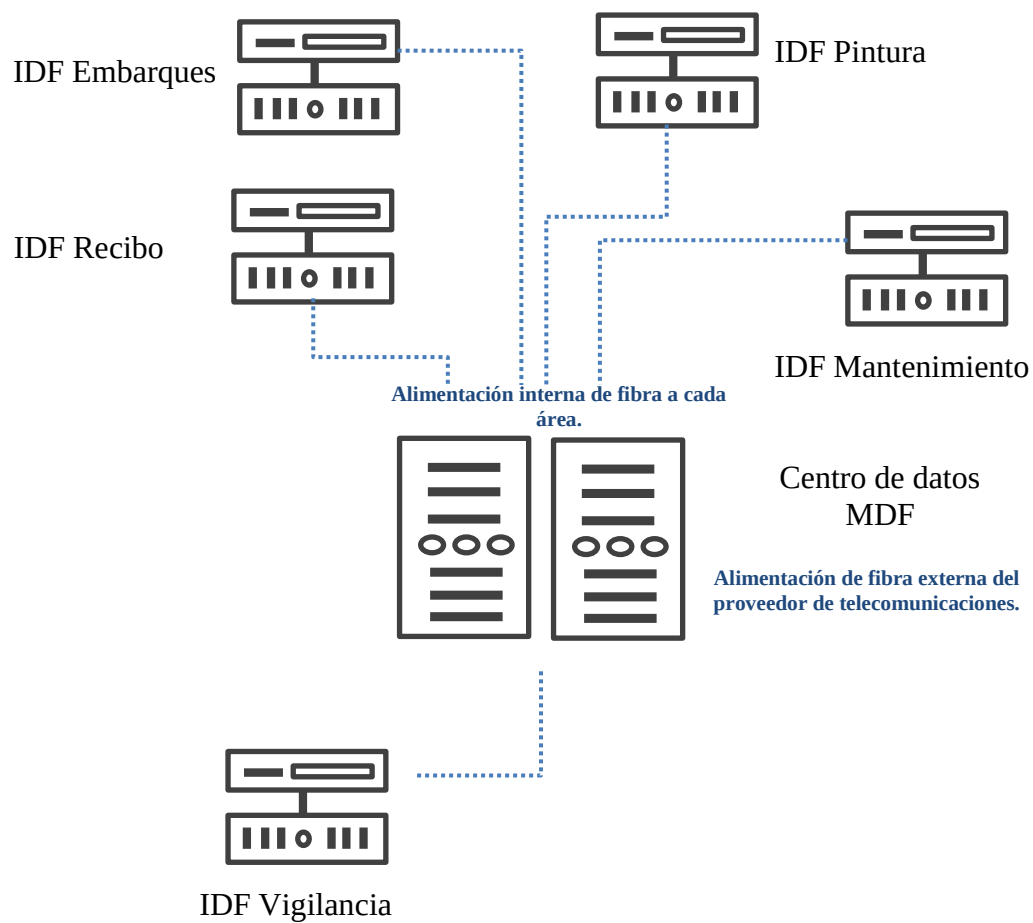


Figura 13 Distribución física IDF en planta (NAVE 1 ENSAMBLES).

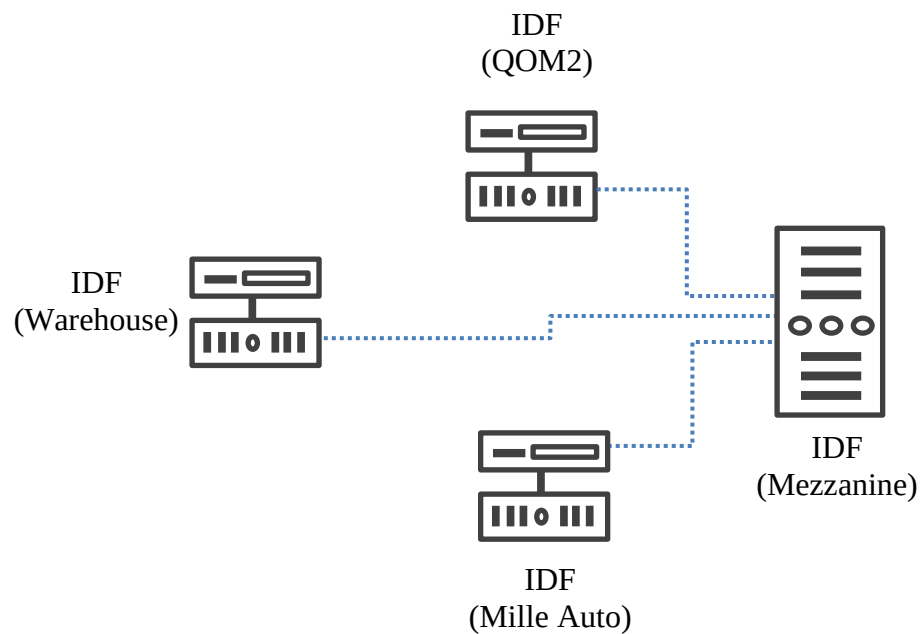


Figura 14 Distribución física IDF en planta (NAVE 2 BREAKERS).

A partir de la Figura 13 es la primera área que denota la sección 2 o mejor conocida internamente como (nave 2), de ahí estos se sustentan de los servicios del centro de datos que dirigen a intercomunicar a los cinco IDFs de la nave denominada (ENSAMBLES), justo se plasma el mismo proceso en la Figura 14 dirige una sola conexión que va adherida al centro de datos hacia la nave 2 (BREAKERS), en donde la nave 2 cuenta con una sala donde también existe un IDF, en la zona alta del mezanine para proporcionar comunicación a toda esa área de esa misma sección.

A continuación, se observan todas las imágenes de los IDF véase en las Figuras 15-23, representan la infraestructura de comunicación física en planta en sus respectivas ubicaciones, cabe mencionar que solo se muestra un antes de implementar el equipamiento de la línea APC. En cada una de estas imágenes se muestran las decadencias de UPS, monitoreo visual, y monitoreo ambiental, que son prácticamente tres bosquejos que abordar en cada IDF, cabe resaltar que no están contemplados los IDFs para alterar la estructura del rack como lo que aplica para los racks del centro de datos en base a las manijas, pero si para automatizar su seguridad desde el monitoreo visual y ambiental.



Figura 15 Identificación de IDF-1 Vigilancia (Surveillance).



Figura 16 Identificación de IDF-2 Embarques (Shipping).



Figura 17 Identificación de IDF-3 Recibo (Receiving).

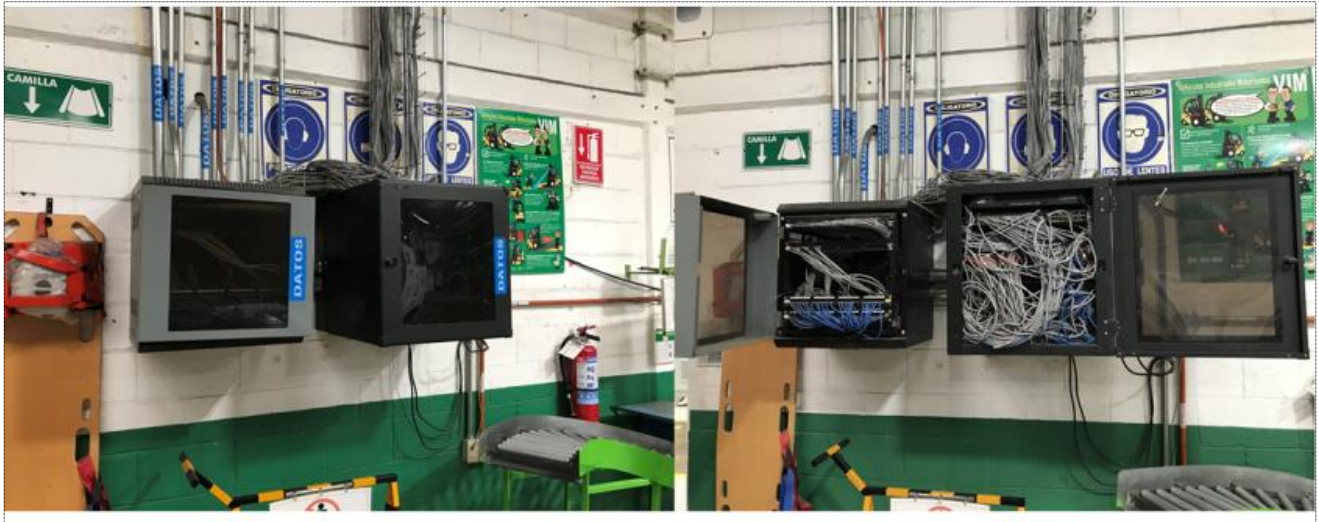


Figura 18 Identificación de IDF-4 Pintura (Paint).



Figura 19 Identificación de IDF-5 Mantenimiento (Maintenance).



Figura 20 Identificación del IDF-6 QOM2 BRK.



Figura 21 Identificación de IDF-7 Mille Auto BRK.

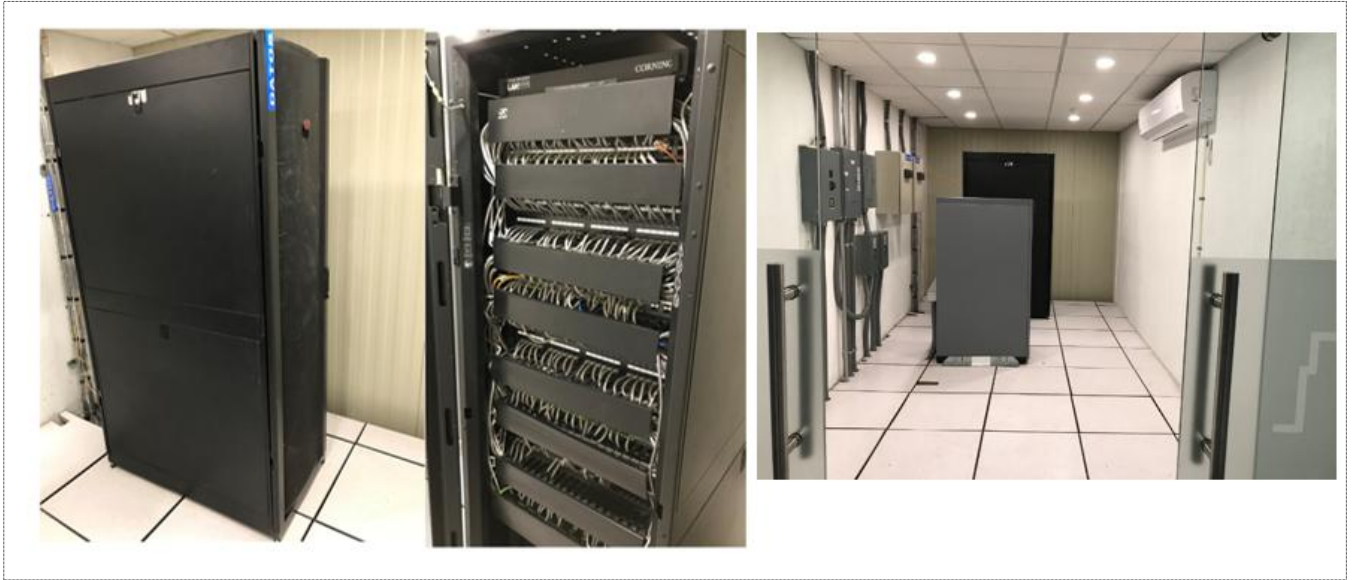


Figura 22 Identificación de IDF-8 Mezzanine BRK.

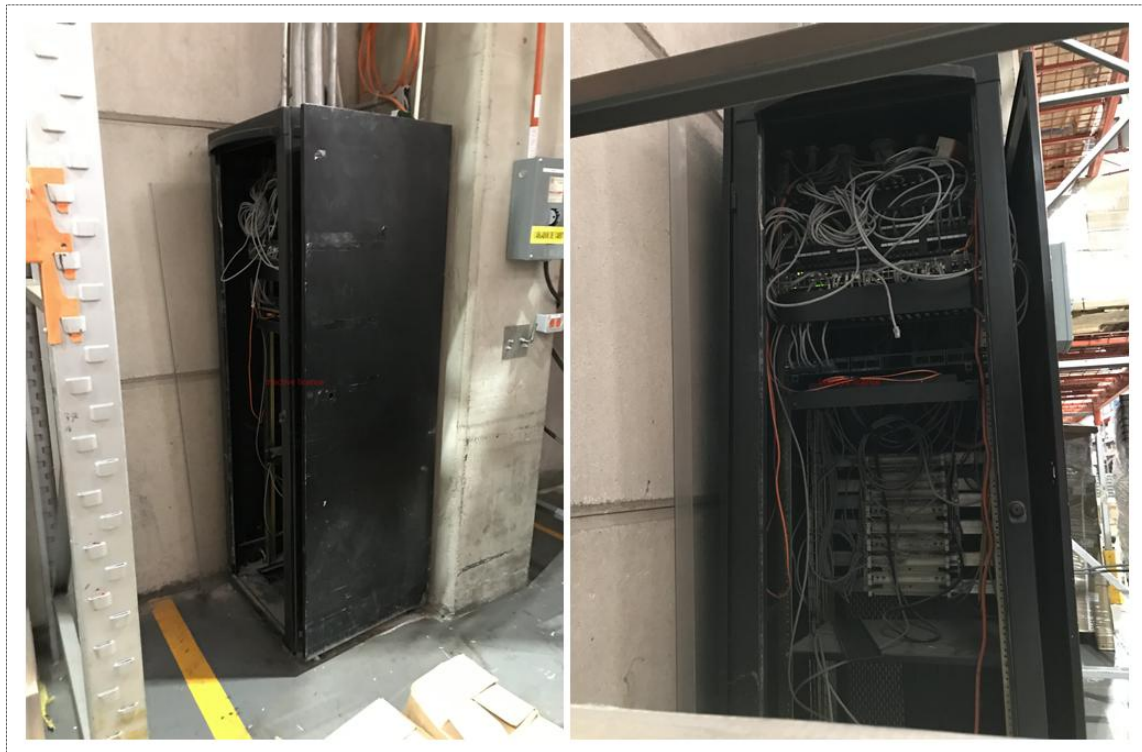


Figura 23 Identificación del IDF-9 Almacen Breakers (Wharehouse BRK).

Por último (Véase Figura 23) en este IDF se puede observar un rack básicamente deteriorado donde su infraestructura interna está mal posicionada, por ende, en este rack se considera, la intervención a la gestión y de decisión interna como la renovación física, el cambio del rack, la estructura y montaje de cableado, donde finalmente se eligió a proveedor para su colaboración en conjunto para algunos sitios, principalmente para armonizar el equipamiento del IDF, y finalmente para ayudar a las óptimas operaciones físicas.

El IDF y su funcionamiento descriptivo

Cuadro de distribución intermediario mejor conocido por sus siglas en inglés, (IDF) es sencillamente un bastidor independiente, que puede ir montado en una pared para administrar e interconectar un cable de telecomunicaciones entre los dispositivos del usuario final, en la arquitectura el IDF está conectado por medio de cables de conexión cruzada vertical (VCC) y conectado con el cuadro de distribución principal (MDF) actúa a su vez como puerta de enlace entre los cables privados o públicos, de la red propia de la planta.

Los IDF son sumamente necesarios en la instalación de toda la integración de la cadena de redes, puesto que son grandes auxiliares, porque son un punto de distribución para cables multipares desde el marco de distribución combinado (CDF) a cables separados que se conectan a dispositivos ubicados en diferentes zonas, la sencilla forma de hacer estas interconexiones permiten conectar cables al MDF y lograr crear una LAN y de ahí partir en organizar cables y reforzar una topología de red ordenada. Los IDF son más utilizados en espacios de dimensiones grandes básicamente para estar ocupado en el coworking.

Dentro de la infraestructura tangible que representan los IDF en planta se toman en consideración por ser dispositivos de alto valor de información y de estos se abarca la mayor parte de la profundidad de la resiliencia, por ende, estos son un conjunto de equipos generalmente estandarizados, pero muchos de estos no logran cumplir ciertos criterios de la estructura de cableado y menos en automatización. La estructura correcta y requerida está basada para distribuir los cables, a equipos que son capaces de prevenir la extinción de incendios por sobrecalentado por medio de sensores, vitales en un área cerrada llena de cables, y algunas veces también medidas de vigilancia.

Los IDFs están integrados por un enrutador, el funcionamiento del enrutador actúa como un servidor para la LAN solo del área establecida, este actuando así como procesador del control de datos, e interviene en dirección a la gestión de puntos de acceso inalámbricos y a su vez la actuación como cortafuegos, los IDF en planta están equipados con dispositivos de copia de seguridad, como unidades de disco duro o de una matriz redundante de discos independientes (RAIN), otorgando la garantía que las estaciones de trabajo requieren. Por lo tanto, es fundamental que los dispositivos y equipos de cada zona cuenten con una copia de seguridad confiable de sus datos.

Esto evidentemente va a permitir la funcionalidad de manera adecuada, son necesidades primarias, que proporcionan funcionalidad y resolución a problemas emergentes. Por mencionar a los sistemas de alimentación ininterrumpida (UPS), que proporcionan energía de emergencia a los equipos

esenciales, y simplemente emergen de un corte de energía, de ahí su funcionalidad de respaldo de corriente eléctrica para los IDFs.

Claramente en estos IDFs hay exposición para padecer de cualquier tipo de percance o riesgos, como: humedad, incendio, sobrecalentamiento, o solo por mencionar alguno de estos, de ahí la llamada prevención de incidentes, en base a los criterios y comienzos de la resiliencia se estipula cubrir todo tipo de necesidades primarias.

El funcionamiento de la seguridad operativa en el hardware

La seguridad física, es resaltar los diferentes métodos utilizados, mayormente preventivos y de detección para proteger físicamente cualquier recurso del sistema, estos recursos van desde lo más básico y esencial pudiendo ser un simple teclado, un CPU, hasta una cinta de respaldo que contiene toda la información de un sistema. Es importante contemplar la seguridad en varios ámbitos en el entorno donde los sistemas físicos y lógicos se complementan y juegan un papel importante dentro del negocio. Tomando en cuenta únicamente el rubro de la seguridad operativa en el hardware se enfoca en las acciones y medidas establecidas para asegurar que los sistemas de hardware de una empresa trabajen de forma segura y sin contratiempos no deseados. Esto implica resguardar el hardware de posibles peligros, y debilidades que puedan poner en riesgo su integridad, disponibilidad y confidencialidad.

En este punto actualmente se generan recorridos continuos dentro de la planta para la verificación del estatus correcto de los dispositivos como equipos de cómputo, servidores entre otros.

A continuación, se menciona cuatro aspectos más que integran la importancia de la seguridad del hardware:

1. Actualizaciones y mantenimiento: Es crucial mantener el hardware al día con las últimas actualizaciones de seguridad y parches de software para protegerlo contra vulnerabilidades conocidas.
2. Monitoreo y gestión de riesgos: Supervisar activamente el hardware para detectar posibles amenazas o comportamientos inusuales, y tomar medidas para mitigar estos riesgos.
3. Respaldo y recuperación: Implementar medidas regulares de respaldo para garantizar la disponibilidad e integridad de los datos en caso de fallos del hardware o ataques cibernéticos.
4. Disposición segura: Al finalizar su ciclo útil, asegurar la eliminación segura del hardware para prevenir filtraciones de datos confidenciales o información delicada.

Comprendiendo esto y aplicado al término resiliencia del hardware se refiere a la capacidad de garantizar la función adecuadamente ante cualquier eventualidad para proteger los activos empresariales. Los siguientes rubros más generales se centran en cubrir criterios y reforzar la seguridad.

Acceso físico

En cualquier sitio de trabajo, se establecen enfoques que implican asegurar el hardware básicamente contra accesos no autorizados, robos, daños accidentales o intencionales, así como garantizar la integridad de los cables y conexiones. El hardware es un referente claro de la implementación de medidas para proteger y controlar situaciones imprevistas que podrían causar daños físicos a los dispositivos informáticos. Solo por hacer mención algunas de estas amenazas visibles incluyen: golpes, caídas, condiciones climáticas adversas, incendios y otros tipos de incidentes. En este contexto, es fundamental no solo proporcionar los elementos de protección adecuada, sino también capacitar a los empleados continuamente para que utilicen los equipos de manera correcta dentro de la planta.

Restringir el acceso físico y lógico al hardware únicamente a personal autorizado es un requisito interno clave, ya que limitar los accesos contribuye a una mejor gestión de la seguridad interna. Para ello, se busca integrar sistemas de control de acceso físico, como cerraduras, alarmas y tarjetas de proximidad, junto con un sistema de monitoreo inteligente.

Desastres naturales

En esta vida nos encontramos diversas situaciones de posibilidades, al igual que esas situaciones donde las circunstancias son inciertas lamentablemente los sistemas también sufren consecuencias. Los eventos más comunes que suelen suscitarse en la región son tormentas eléctricas que generan cortes de flujo eléctrico, inundaciones, filtraciones de humedad, y el humo, hoy en día son un problema que si afecta a la infraestructura de la planta.

Hablando de un posible escenario crítico, la ubicación de la planta se sitúa en una zona sensible a movimientos tectónicos (temblores), previamente tomando esos factores en cuenta la planta ha sido resguardada en la integridad de su información haciendo respaldos y migrando información valiosa a la nube como parte de un protocolo de seguridad y resguardo de información, de igual manera considerando estas medidas en un evento catastrófico como un incendio o un terremoto en el peor de los escenarios. Los desastres naturales evidentemente pueden traer repercusiones bastante serias especialmente si no están considerados dentro de una política de seguridad en su implementación.

Evaluación de la comprensión a la exposición al riesgo

Dentro de la evaluación de los equipos TI hay ciertos criterios que dirigen la exposición a los “riesgos”, y hablar de los riesgos es un eje importante para delimitar situaciones sobre esta parte de la infraestructura, existen aspectos que son importantes y hacerlos notar es un claro ejemplo de cómo fundamentar este trabajo, los riesgos y problemas si existen en la infraestructura y en la lógica de los funcionamientos de los sistemas. La ciberseguridad es otra área integrante que ya se mencionó con

anterioridad al inicio de este proyecto, que se encarga de monitorizar, controlar, y prevenir los riesgos y lograr hacer de los sistemas más resilientes a nivel software.

Todos estos factores van asociados al desempeño de la organización, y es totalmente considerado en la implementación de este proyecto, que claramente se tiene la intención de reducir el impacto de una exposición u amenaza a la infraestructura que puede producir una interrupción física o a los servicios que la infraestructura ofrece. Dentro de la tecnología se pueden generar factores que den ese impacto a la infraestructura, como lo que pueda llegar a suscitar en debidas ocasiones y pueda hacer que restablecer un servicio se vea acomplexado o que de igual manera requiera de un soporte y puede estar asociado con vulnerabilidades y riesgos, a lo que este aspecto se refiere es que una parte de ello pueda relacionarse internamente en la planta desde usuarios, proveedores, visitantes entre otros. En el caso de los proveedores suelen ser recurrentes sus servicios en planta, los cuales deben dar cierto tipo de soportar a procesos importantes, por ende, logran acceder a sitios físicos de información, por lo cual también pueden representar un riesgo. Si se piensa en el riesgo como tal, se desglosan otros factores de alcance mundial, como es el caso de los ataques de datos, si ya se habla de vulnerabilidad en la infraestructura el ataque a datos es el mayor riesgo y más temido de toda la industria.

Para la infraestructura física es claro que se dirige a otro tipo de mención de riesgo, más conocido y comprendido como un tema de “seguridad” como la mención con el tema de proveedores, visitantes etc., todo riesgo va de la mano con más aspectos de vulnerabilidad que están presentes. Para crear resiliencia, es fundamental empezar por cambiar las ideas sobre los riesgos y amenazas, porque solo así se puede consolidar la parte de TI y el negocio, es como generar aspectos productivos para identificar los beneficios que se darán al mitigar riesgos que son resumidos en parte en temas de “seguridad”, y dar paso a una estrategia que a su vez utiliza un lenguaje común para dar soluciones con recursos físicos. Con base a ello el análisis permite tomar buenas decisiones que conllevan a acciones inteligentes e informadas sobre cómo gestionar los riesgos y amenazas.

El desfasamiento del hardware en la infraestructura

Con la constante agilidad de la tecnología hoy en día los sistemas evolucionan, y de algún modo con el paso del tiempo los recursos físicos se vuelven más obsoletos debido a algunos cambios que pudiesen estar en sus componentes, claramente es así, porque la innovación tecnológica nos obliga a adaptarnos a los requerimientos de la fluctuación incesante. Una infraestructura de TI desactualizada u obsoleta puede generar una conectividad deficiente, velocidades de procesamiento lentas y almacenamiento de datos frustrantes. El no enfocar la arquitectura de la infraestructura informática a procesos de renovación genera susceptibilidad, es decir, el no manejar de forma óptima todo el software y hardware, entorpece los procesos de comunicación en donde se recopila, almacena y gestiona la información.

Principios de reducción a los riesgos

Para poder contribuir a la protección ante los riesgos tecnológicos es a partir de la ejecución de un plan íntegro que promulgue la gestión de riesgos, este, en un conjunto de políticas y prácticas que se aplican a nivel estructural, cubriendo así, los dispositivos y datos de la organización.

Dentro de las responsabilidades internas TI, implica identificar y analizar los retos y amenazas como parte de la gestión de riesgos en los que se pueda enfrentar la empresa, gestionando de forma proactiva estos riesgos mediante la implementación de estrategias y creando acciones de contingencia. Una de las cuestiones que principalmente se tiene en cuenta para mitigar, es el plan de reducción de riesgos en la infraestructura, cuya gestión permite emplear los siguientes principios que se aplican en este proyecto:

- Mantener la funcionalidad en cuanto a los servicios en la duración de la afectación de la infraestructura tecnológica, esto es mejor conocido como resiliencia operativa.
- Brindar referencia oportuna a los usuarios, cumpliendo con sus expectativas en el uso de los servicios soportados por TI en la empresa.
- Establecer comunicación entre los equipos de servicios TI que influyen para el funcionamiento correcto del entorno empresarial como: administradores de TI y los proveedores que brindan los servicios a la planta, o simplemente el escalamiento de la situación a otro team de soporte por medio de un sistema de tickets.
- Enfocar y desarrollar aptitudes de competencias en los administradores de TI, para responder a los planos de contingencia y continuidad a los procesos que se vayan desarrollados.
- Establecer la comprensión sobre acciones ante las vulnerabilidades y las ciertas amenazas a los que se pueden exponer los servicios tecnológicos infraestructurales y lógicos.

Requerimientos para la mejora del servicio TI en infraestructura

Reiteradamente se habla de la seguridad, el mantener un servicio activo bajo sus operaciones es un factor repetitivo de querer automatizar ciertos aspectos físicos tecnológicos, e insistentemente de la mejora continua a la infraestructura TI, son prioridades tomadas para este tema. Está de por medio el comprender fijar necesidades faltantes, y es relevante desde la idea principal que permite plantear el desarrollo de este trabajo.

Dentro del análisis, en cada junta se desarrolló plantear necesidades, y aquellas cadencias que tiene la infraestructura. En este caso se pide tomar únicamente ciertos criterios y ciertas necesidades que requieren algunas zonas de la infraestructura.

- Comenzando por el Centro de Datos (site). Se toma como necesidad primordial el cambio de acceso a los rack de los servidores, esto porque en ellos se dispone de esa característica que se menciona antes, reiterando que cumplan con la estructura adecuada, como el tipo de rack para que sea adaptable a los requerimientos, aquí se busca cambiar el tipo de acceso hacia los

gabinetes (racks) y esto aplica también para el rack del Mezzanine, en ellos implementan la automatización en puertas y chapas, pero a su vez con un modelo de mejoría en su monitoreo como la implementación de sensores .

- En la segunda posición es monitorear el resto de los IDFs. Estos están contemplados para ser automatizados únicamente con la integración basada en el monitoreo y su registro de estado mediante sensores.

Procesos de gestión de resiliencia en la infraestructura TI

Como todo proyecto siempre se abarca una gestión de trabajo, la resiliencia en la infraestructura a menudo se asocia con la capacidad que tiene la infraestructura física o del sistema físico para hacerle frente a la efectividad de las estrategias que contribuyen a una organización resiliente. La incorporación de sistemas de monitoreo visual, ambiental, y los sistemas de alimentación ininterrumpida sirven de ayuda a la infraestructura para hacer frente a las amenazas/riesgos y recuperarse de eventos disruptivos, simplemente no se logra sin una base organizativa que sea capaz de afrontar y responder a las crisis, comenzando por la estrategia que es parte de los procesos que complementan las acciones que se toman en consideración para implementar la mejora en la automatización, y al mismo tiempo prevención, con lo cual se pueda mantener activo estos tres principios de gestión que son asociados a la implementación de la resiliencia.

Gestión de la seguridad

Retomando el criterio mencionado al plan de reducción de riesgos, es sumamente importante garantizar y poner en práctica los procesos y metodologías que la organización requiera para su protección donde pueda ser implementada la seguridad con el fin de protegerse y garantizar la protección de sus activos e información confidencial, privada o sensible frente a las amenazas o aquellos aspectos de riesgo que puedan ser intervenidos como ataques internos o externos, divulgación, destrucción o modificación.

Gestión de la continuidad del negocio

Con toda la información recopilada el desarrollar planes de continuidad dentro y fuera de la planta es mantener siempre vigente el compromiso de la prevención en la organización general, manteniendo el funcionamiento con un nivel mínimo aceptable durante una contingencia, en cualquier aspecto que involucre un desequilibrio en las operaciones o bien sea por un desastre natural, corte en suministro, fallo en sistemas, sabotajes, etc., todo esto con el fin de mantener toda una estrategia y alcanzar los objetivos iniciales de la organización. La ventaja va acorde de considerar un marco para la continuidad

del negocio, que es la ayuda a las organizaciones a sobreponerse ante amenazas que puedan interferir en su operación normal.

Gestión de la operación de TI

La gestión eficaz de la continuidad del negocio internamente en la planta es todo aquello lo que enlaza lo ya mencionado, y significa que la organización puede reanudar las operaciones y volver a operar el negocio como lo hace habitualmente en tiempos más rápidos. Mantener el negocio es reinventar las ideas y pensar en dar estrategias para implementar esa seguridad, logrando llevar siempre a las mejoras de las infraestructuras tecnológicas y complementarlas con sus activos en su parte lógica, generando así, el llamado de sistemas resilientes continuos.

En función de lo ya mencionado es prioritario destacar que para gestionar algo e implementarlo se debe de potencializar los recursos que se encuentran funcionando en el entorno de la infraestructura, ya sean dirigidos en pequeños proyectos o proyectos de mayor amplitud. Por lo tanto, los procesos de gestión son destacables al abarcar los principios fundamentales de control, los cuales se desglosan en los siguientes aspectos:

Seguridad del espacio físico y factores del entorno.

- El disponer y generar los permisos como; el control de accesos a los sitios que concentran activos, el monitoreo muestra los tiempos de vigilancia del personal entrante y saliente, esto al mismo tiempo genera protección de los activos frente a daños o robo. Aquí se dispone de acceso a ciertas áreas con tarjetas de proximidad.

Gestión a las comunicaciones que se producen con el monitoreo

- La recolección de información que proporcionen los dispositivos inteligentes se recauda a partir de los sensores, como la, temperatura, humo, humedad permite establecer esa conectividad de todos los aspectos técnicos y de carácter administrativo que le permiten a la operación el funcionamiento correcto de los activos.

Adquisición, desarrollo y mantenimiento de sistemas de información.

- En palabras cortas es abarcar todo el proceso de vida de los sistemas de información, desde la adquisición inicial de los dispositivos, hasta su utilización constante y mantenimiento a lo largo del tiempo de su existencia vigente.

Gestión de incidentes en la seguridad de la información.

- Aplicación de acciones preventivas, y correctivas que puedan presentarse en los activos.

El Cumplimiento

- Asegurar el cumplimiento de los estándares técnicos y las regulaciones vigentes y pueda incidir directa o indirectamente sobre el tratamiento de la información.

Estándares de normatividades de la continuidad empresarial

Como ya se ha ido mencionado al inicio de este trabajo hay factores que se involucran dentro de un plan de abordaje que describe un marco de la normatividad de contribuir al compromiso de desarrollar un plan continuo para el negocio y cuyo enfoque se describe en el (Plan de acciones). Tomando esto en relevancia, la planta y la misma organización en general cuenta ya con distintas normas llamadas ISO, son un conjunto de normas de control de calidad y gestión de calidad, establecidas por la “Organización Internacional de Normalización”. Cuyas normas le permite a cualquier tipo de organización sea grande, mediana o pequeña tener certificación de acuerdo con la actividad en la que esté orientada a la producción de bienes o servicios. Schneider Electric ya es acreedora de muchas de estas normatividades y a su vez busca que con el modelo resiliente cubra las necesidades normativas. Solo por mencionar algunas de las normas ISO más habituales que aplican para la intervención de la resiliencia inteligente y al enfoque dirigido a las TI puesto que ellas impulsan la mejora de los servicios tecnológicos.

A continuación, se menciona manera resumida de algunas de las normas ISO más importantes que cuenta la organización basada en seguir con el cumplimiento de los estándares tecnológicos.

ISO 22301 (Plan de continuidad de negocio)

Basándonos en la norma ISO 22301 y siguiendo este estándar es la primera norma internacional que se considera el único marco creíble para la gestión eficaz de la continuidad del negocio en el mundo. Esta se ha desarrollado para ayudar a las empresas a minimizar el riesgo del tipo de interrupciones que en ellas ocurren. La gestión de la continuidad del negocio se asegura de que una empresa pueda seguir funcionando mientras se recupera del desastre. La normativa exhorta a las empresas a seguir un conjunto de procedimientos y controles destinados a asegurar que la infraestructura tecnológica pueda continuar funcionando con rapidez, claramente esta señala en reducir el impacto mediante los temas que se han ido desglosando en la parte superior. La ISO 22301 impulsa el cumplimiento de los lineamientos y procedimientos establecidos para evitar interrupciones y persuade en el mejoramiento de la resiliencia con las políticas y herramientas que señala un DRP.

Mientras tanto, el DRP es un proceso de devolver una empresa u organización a un estado de normalidad después de un evento desastroso. Esto normalmente incorporará la continuidad del negocio, pero el enfoque está en la recuperación total.

¿Cuál es la diferencia entre la gestión de la continuidad del negocio y la recuperación ante desastres?

La gestión de la recuperación ante desastres (DRP) suele tener lugar en el contexto de la gestión de la continuidad del negocio. Esto interviene que en los planos de recuperación ante desastres suelen ser relativamente técnicos y son siempre centrados en la recuperación de operaciones, funciones, sitios, servicios o aplicaciones específicas. Las mejores prácticas para la recuperación ante desastres también se establecen en ISO/IEC 22301.

Los beneficios de la gestión de la continuidad del negocio dentro de la norma ISO 22301 es la implementación correcta de la gestión de la continuidad del negocio, reduce la probabilidad de que ocurra el riesgo. Si tal cosa ocurre, entonces la empresa estará lista para responder en consecuencia, reduciendo así significativamente el daño y obteniendo benevolencia.

Las diversas necesidades de clientes, accionistas y trabajadores se abordan de manera oportuna a través de una correcta evaluación de riesgo como:

1. Reducir el tiempo de inactividad ante cualquier amenaza, en este caso, se incluye el tiempo de recuperación. Así, se obtienen beneficios laborales, de tiempo y financieros, se reducen costos y se incrementan los resultados financieros de la empresa.
2. El aumento a la productividad de la planta genera que se siga brindando asistencia de emergencia bajo amenaza.
3. La reputación de la empresa genera valor de marca y mejora de la reputación, fortaleciendo su brazo en competencia.
4. La cadena de suministro de la empresa se vuelve más segura, se cumple con las solicitudes legales y se crean nuevas oportunidades y la confianza del cliente.

Ante esta norma la organización podrá restablecer el trabajo normal lo más rápido posible en caso de fuerza mayor o situación de crisis. La norma ISO 22301 garantiza el trabajo ininterrumpido, la perfección del sistema de gestión, la disponibilidad de tecnologías científicas modernas, etc., lo que favorece la imagen de la empresa y le permitirá alcanzar un nivel completamente nuevo.

ISO 27031 (Preparación de las organizaciones ante incidentes de interrupción de los servicios de tecnología de la información TI)

Esta ISO enfoca a las mejores prácticas evolutivas de las TIC's y está marcada por directrices para la preparación de las TI basadas en el cumplimiento de la continuidad del negocio. El estándar internacional para la gestión de la continuidad del servicio de tecnología de la información y la comunicación TIC, forma parte de la familia de estándares ISO 27001 para la seguridad de la información. Se hace de ella mención porque incentiva que las organizaciones desarrollen procedimientos de continuidad del negocio para respaldar su sistema de gestión de seguridad de la información (SGSI).

El estándar ISO 27031 proporciona recomendaciones adicionales específicamente para la gestión de la continuidad de las TIC's al alinearse con las normas ISO 27001 o ISO 22301 y cubre todos los eventos e incidentes (incluidos los eventos relacionados con la seguridad) que podrían afectar la infraestructura y los sistemas tecnológicos. Esta ISO no es un estándar certificable, sino una guía de mejores prácticas para lograr la continuidad comercial de los sistemas tecnológicos de la infraestructura.

La norma ISO 27031 es importante para la prevalencia de la información y la comunicación entre equipos tecnológicos ante la recuperación de eventualidades desagradables, siempre situada ante la gestión de continuidad por los siguientes argumentos:

- Definición estructural empresarial (organigrama).
- Descripción de puestos de dirección y sus respectivas funciones.
- Información de contactos y claves de clientes.
- Layout y descripción de instalaciones en planta.
- Ubicaciones e inventarios de equipos informáticos software/redes.
- Información de recursos críticos en situación de emergencia.

Cabe mencionar que estas normas cumplen en la organización únicamente dentro de los sistemas de comunicación lógica y se busca retomar de ellas las mismas pautas, pero para retroalimentar a los sistemas de infraestructura de servicios físicos en la planta, en la cual cuya finalidad se espera ser completada en una segunda fase de su evolución futuro de este proyecto.

Proceso de resiliencia en infraestructura TI basados en los dispositivos automatizados

Schneider Electric cuenta con una línea de productos tecnológicos que son distribuidos a nivel mundial. APC (American Power conversion) es una submarca de la familia de Schneider Electric que se enfoca en proporcionar soluciones tecnológicas.

APC es la creación de una línea de productos relativamente desconocida pero ya existe desde hace muchos años en el mercado, su importancia va dirigida para la optimización y simulación de procesos complejos y es extremadamente relevante en sectores que requieren optimización muy precisa de lazos de temperatura, presión/caudal, por lo cual su producto principal es relacionado con la alimentación eléctrica y la gestión energética para equipos electrónicos. Actualmente en su producción ha integrado una línea más amplia para la gestión de la seguridad a partir de nuevos productos. APC es una marca comercial y puede ser adquirida para el uso específico de integración y optimización de recursos tecnológicos automatizados.

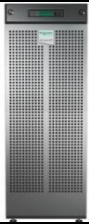
Las soluciones que ofrece son múltiples y pueden ser implementadas con herramientas físicas que en este caso disponen de hardware, y se complementan con servicios lógicos como firmware, y el software, estos funcionan a partir de su propio sistema de control, que consiste en integrar dispositivos y dar comunicación, por medio de una interfaz de usuario en tiempo real (UI/UX).

En la (Tabla 2) se detallan los aspectos más relevantes que abordan las necesidades de la infraestructura, así como los dispositivos que proporcionan seguridad y satisfacen las demandas tecnológicas. Se presentan cada uno de estos componentes considerados para la intervención con el objetivo de prevenir, mejorar y automatizar todos los aspectos tecnológicos que lo requieran. Estos elementos son fundamentales para justificar una adecuada implementación y comprensión de la resiliencia. Schneider Electric ofrece soluciones basadas en sus propios productos, buscando lo más completo de la industria como medidas para la seguridad de TI. Por lo tanto, el uso de este tipo de dispositivos tecnológicos representa una transformación significativa en la infraestructura.

Tabla 2. Lista de aditamentos APC requeridos para la implementación.

Nombre	Serie	Imagen del producto
Unidad Smart-UPS X de APC, 1500, 1440 VA, 120 V, LCD, montaje en bastidor / torre, 2U, 8 tomacorrientes NEMA 5-15R, con puerto SmartConnect (3 unidades)	SMX1500RM2UC	
Armazón de batería de funcionamiento prolongado PX 40KW con 8 módulos de batería y puesta en marcha (1 Unidad)	SYCFXR8-8	
Paquete de baterías externas para rack / torre de APC Smart-UPS serie X, 48 V, 864 VAh, montaje en rack, 2U. (9 unidades)	SMX48RMBP2U	
Unidad Smart-UPS SRT de APC, 5000, 5400 VA, 208 V, LCD, montaje en rack con kit, 2 tomacorrientes. (1 unidad)	SRT5KXLT	
Unidad Smart-UPS SRT de APC, 5000, 5400 VA, 208 V, LCD, para montaje en bastidor, 3U, 2 tomacorrientes. (7 unidades)	SRT5KRMXLT	

Paquete de baterías APC Smart-UPS SRT (5 kVA y 6 kVA) 192 V, 1920 VAh, montaje en rack con kit. (2 unides)	SRT192BP	
Paquete de baterías APC Smart-UPS SRT (5 kVA y 6 kVA) 192 V, 1920 VAh, montaje en rack, 3U (12 unides)	SRT192RMBP	
Monitor de sala NetBotz 755 (8 unidades)	NBWL0755	
Sensores de interruptor de puerta (NetBotz) para un rack APC - 12 pzas. (6 unidades)	NBES0303	
Monitor de rack (NetBotz 750) (3 unidades)	NBRK0750	
Módulo de cámara 165 (NetBotz) (5 unidades)	NBPD0165	
Sensor inalámbrico de temperatura y humedad (NetBotz) (7 unidades)	NBWS100H	
Kit de mango (chapas inteligentes) (7 unidades)	NBHN125	
Sensor de cuerda extensor (1 unidad)	NBES0308	
Sensor de humo (3 unidades)	NBES0307	
NetBotz Rack Access Pod 175 125 Kit (extensor). (1 unidad)	NBPD0125	

Regleta PDU (2 unidades)	AP9567	
Tarjetas de proximidad APC (10 unidades)	AP9370-10	
MGE Galaxy 3500 30kVA 208V con 4 Módulos de Batería, Arranque 5X8 (1 unidad)	G35T30KF4B4S	
Gabinete para servidores NetShelter SX de APC 42 U, 600 mm x 1070 mm, con paneles laterales. (3 unidades)	AR3100	
Back-UPS APC 700 (9 unidades)	BR700G	

La Tabla 2 presenta una lista de dispositivos de primera calidad que aportan confiabilidad al negocio gracias a su avanzada tecnología. Esta lista incluye aditamentos complementarios necesarios para la instalación adecuada de los dispositivos principales, lo que asegura el correcto funcionamiento de cada uno. Asimismo, esto permitirá que el monitoreo se realice de manera efectiva.

Se hace especial énfasis en algunos dispositivos destacados en la lista; sin embargo, esto no resta importancia a los demás dispositivos que también serán implementados. Solo un par de dispositivos desempeñan el papel de operadores centrales primarios para gestionar el monitoreo.

IMPLEMENTACIÓN TECNOLÓGICA

Descripción inicial de los dispositivos

NetBotz Room Monitor 750

Este dispositivo (Véase Figura 24) es fundamental debido a su función de monitoreo y control ambiental, lo cual resulta esencial para la seguridad física de la infraestructura. Se trata de un hardware diseñado específicamente para la supervisión.

“El NetBotz está diseñado para brindar protección contra amenazas ambientales y riesgos de acceso no autorizados que pueden causar tiempo de inactividad en la infraestructura de TI, tanto en entornos Edge Compute como en centros de datos.” Dispositivos de seguridad APC (s.f).

Este dispositivo integra componentes como sensores, controles de acceso compactos y cámaras HD, cuya funcionalidad se centra en la protección de entornos mediante vigilancia y alertas flexibles configurables por el usuario. Su propósito es mitigar riesgos asociados con daños por agua, altas temperaturas, humedad, incendios u otras condiciones que puedan afectar aplicaciones críticas para la empresa. Además, cumple con las normativas vigentes y automatiza el monitoreo, facilitando la identificación y vigilancia del acceso a racks a través de sus dispositivos integrados.

El objetivo principal de estos dispositivos es mitigar riesgos mediante el uso de su amplia gama de sensores compatibles, lo que les permite capturar y almacenar clips de cámara, así como generar alarmas configurables.



Figura 24 NetBotz Room Monitor 750.

En la Figura 24 se muestra como un dispositivo primario. Ya que su funcionalidad está en administrar los demás dispositivos que se interconectan en ellos. Véase sus características y ventajas en Tabla 3.

Tabla 3. Descripción de características y ventajas del dispositivo NetBotz 750 en su implementación.

Características	Ventajas
Soporte nativo para sensores inalámbricos	Gestión de hasta 47 sensores de temperatura/humedad de manera inalámbrica desde un solo NetBotz
cumplimiento normativo	Los accesorios (kits) de manejo de acceso a los racks proporcionan una ruta de auditoría sobre quiénes acceden a las carcassas para que la organización pueda cumplir fácilmente con las pertinentes normativas en materia de protección de datos.
Administración remota	Detección y grabación de movimiento que permite la asociación de un registro visual con una alerta de acceso o ambiental, lo que acelera el proceso de análisis de las causas fundamentales.
Control de acceso físico	Concesión de acceso autorizado del personal al equipo mediante la autenticación de tarjetas de proximidad.

NetBotz Wall Monitor 755



Figura 25 NetBotz Wall Monitor 755.

La Figura 25 muestra un dispositivo de alta supervisión, al igual que el modelo 750, está destinado para ser implementado a salas y espacios tecnológicos que ocupen ser monitoreados en los entornos que así lo requieran, posibilitando así la detección de una alerta de acceso, ya integrado con un sensor ambiental, lo que permite el control y monitoreo del estatus de forma unificada. (Véase Tabla 4) características y ventajas del dispositivo.

Tabla 4. Características y ventajas del dispositivo NetBotz 755 en su implementación.

Características	Ventajas
Soporte nativo para sensores inalámbricos	Gestión de hasta 47 sensores de temperatura y humedad inalámbricamente con distribución de comunicación directa con NetBotz 750
cumplimiento normativo	Los accesorios (kits) de manejo de acceso a los racks proporcionan una ruta de auditoría sobre quiénes acceden a las carcasas para que la organización pueda cumplir fácilmente con las pertinentes normativas en materia de protección de datos.
Administración remota	Detección y grabación de movimiento que permite la asociación de un registro visual con una alerta de acceso o ambiental, lo que acelera el proceso de análisis de las causas fundamentales.

Supervisión	Concesión de acceso autorizado del personal al equipo mediante la autenticación de tarjetas de proximidad.
--------------------	--

Seguridad y monitoreo ambiental es lo que representan este dispositivo llamado NetBotz de la línea APC. Ambos dispositivos son una solución totalmente escalable para resguardar equipos de TI, sensibles contra ataques físicos, tales amenazas como; altas temperaturas, daños por fluidos y accesos no autorizados.

A continuación, se presenta una imagen que ilustra la compatibilidad del dispositivo NetBotz 750 con los dispositivos NetBotz 755 (Véase Figura 26), destacando las mismas características en cuanto al monitoreo y al uso de sensores inteligentes para la protección de equipos TI.



Figura 26 Compatibilidad y aditamentos del NetBotz 750 y 755.

Ambos dispositivos de supervisión funcionan como un equipo de hardware centralizado, diseñado específicamente para operar en un sistema de seguridad y monitoreo de un entorno específico. Esto significa que cada dispositivo cuenta con características particulares en su estructura para lograr optimizar y satisfacer los requisitos de ese entorno tales como:

1. Los puertos polifacéticos ayudan a generar conexiones para los sensores y otros dispositivos de la misma línea del fabricante, en este caso es APC, y de igual manera pudiendo incorporar otros dispositivos de terceros.
2. Puertos que proveen alimentación a otros dispositivos y al mismo tiempo generan control.

3. Integración de módulos de sensores para expandir el entorno de supervisión.

Fase inicial primaria instalación de hardware al centro de datos

Inicializando la etapa de implementación para los dispositivos de comunicación se cubrió la zona principal que es el centro de datos para retomar los puntos del apartado, véase en las Figura 9-11 como la identificación de la infraestructura física interna y sus requerimientos. Se busca abarcar parte de las necesidades con el dispositivo NetBotz 750 de acuerdo con las características periféricas, y físicas de montaje que este dispositivo tiene. (Véase Figura 27).

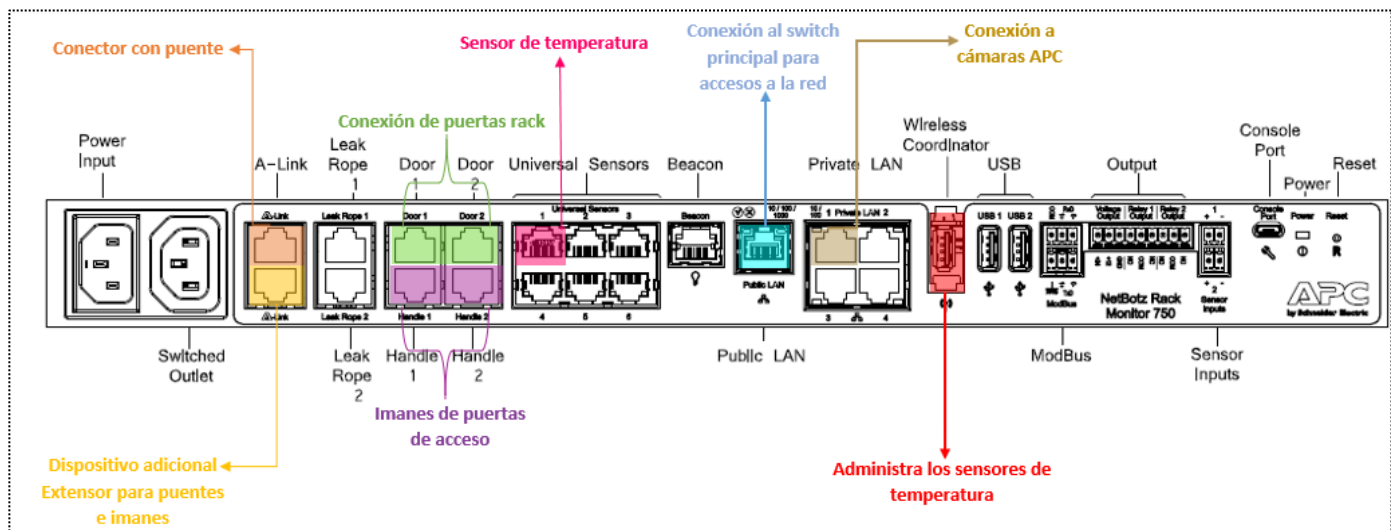


Figura 27 NetBotz Room Monitor 750 y puertos de conexión.

Para comprender (Véase las Figuras 28-29) Room Monitor 750 refiere a la adecuada instalación del dispositivo para su marcha. Donde el montaje se hizo en dos rieles dentro del rack del servidor de manera horizontal. En total se integraron dos NetBotz 750 uno en la parte superior entre los servidores y los UPS, y el segundo en la parte inferior de estos para cubrir más demanda para la conexión de las puertas de los racks.

Respetando las descripciones del cableado de la Figura 27 donde se describe los puertos de conexión utilizados para el arranque del dispositivo, Con base en las consideraciones anteriores, se determinan en reunión los elementos necesarios para la configuración de los dispositivos. El departamento de conectividad se encarga de dirigir la instalación y configuración en cada sesión de dispositivos conectados, preparando así el sistema para futuras intervenciones.

Configuración inicial realizada por el socio técnico (tech partner) a través de una computadora

Para que los dispositivos tuviesen acceso a la red se verifico que la computadora esté configurada para obtener la configuración de red a través de DHCP.

Se hace la respectiva conexión del cable de red desde la computadora a uno de los puertos de LAN privados del NetBotz. Se utilizó un puerto LAN público para conectar el dispositivo a la red.

Abriendo la terminal (símbolo del sistema) se ejecutan ambos comandos:

```
ipconfig /release  
ipconfig /renew
```

La terminal finaliza mostrando una dirección IP, una máscara de subred y una puerta de enlace predeterminada.

A partir de la configuración del sistema, se accede en red e internet y en el cambio de opciones de adaptador, se hace la configuración de red del dispositivo, más a detalle (Véase Tabla 5).

Tabla 5. Opciones de configuración de red en el dispositivo.

Parámetro	Descripción
Estático	Se elige la opción “Estática” para configurar manualmente la conexión a red. Esta opción asignará una dirección IP fija al dispositivo.
DHCP	Se ocupa de un servidor DHCP para configurar automáticamente la red. Esta opción asignará al dispositivo a una dirección IP dinámica.
Nombre del host	El nombre del host del dispositivo.
TCP/IP	
Dirección IP	La dirección IP del equipo, debe estar en formato xxx.xxx.xxx.xxx.
Máscara de subred:	La configuración de la máscara de subred en el dispositivo.

Puerta de enlace	La dirección IP de la puerta de enlace por defecto.
DNS Principal	La dirección IP del servidor DNS primario.
DNS Secundario	La dirección IP del servidor DNS secundario.

Nota: La tabla muestra la configuración inicial de acceso a red para el dispositivo NetBotz por medio de una computadora, y ha sido reescrito para ser expuesto en este proyecto. Fue recopilado de “Installation and Quick Configuration NetBotz” por APC (2022) procedente de: https://www.se.com/es/es/download/document/990-91106_EN/

Una vez puesto en marcha el dispositivo en la red, el equipo de conectividad (redes) toma acción remota del equipo para terminar de hacer las configuraciones, teniendo acceso a través de la interfaz de usuario del NETBOTZ a través de un navegador web, ingresando la dirección IP del dispositivo.

El equipo de redes tiende a fungir como administradores de la red puesto que ellos se encargan en hacer todas las configuraciones necesarias para el funcionamiento de los sensores y cámaras en tiempo real. Posteriormente se trabaja en equipo recibiendo las indicaciones para el montaje de los sensores, estos son montados en base a la configuración que hace el departamento de redes, previamente los sensores cuentan con su propio cable, pero para el resto de las conexiones se hizo y se utilizó cables de conexión Ethernet CAT-5, estos no son excedentes de más 15 metros cada uno.

Primeras instalaciones:

1. Montaje de sensores: 3 sensores inalámbricos de temperatura y humedad NBWS100H (Véase Tabla 2).
2. Montaje de sensores de interruptor de puerta: 3 piezas para puertas de racks NBES0303 (Véase Tabla 2).
3. Montaje de chapas: 4 piezas mangos inteligentes NBHN125 (Véase Tabla 2).
4. Montaje de cámaras APC: 2 piezas NBPD0165 (Véase Tabla 2).



Figura 28 Primer NetBotz 750 (Superior del rack del servidor).



Figura 29 Segundo NetBotz 750 (Inferior del rack del servidor).

En función de las necesidades del centro de datos, se ha implementado una gestión integral de monitoreo y vigilancia. Esto incluye la instalación de cámaras, cerraduras inteligentes, sensores de puertas, así como sensores de humedad, temperatura y humo. Además, en colaboración con el proveedor, se llevó a cabo el reemplazo del rack que almacena el clúster.

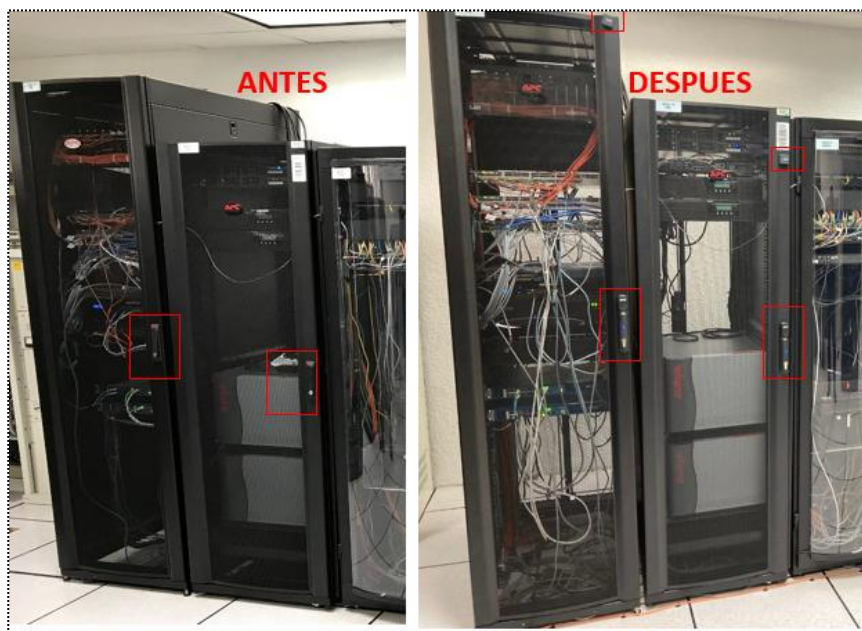


Figura 30 Integración de manijas en racks y sensores de temperatura.



Figura 31 Instalación de sensor de humo, manija interna, e interruptor de puerta.



Figura 32 Implementación de manijas inteligentes.

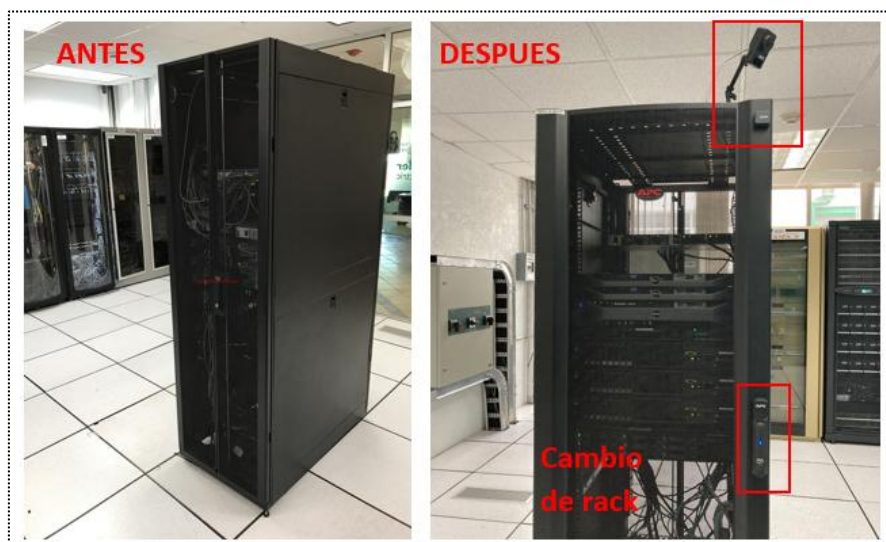


Figura 33 Cambio del almacenamiento del clúster

Tras la instalación de los dispositivos en el centro de datos (Véase Figuras 28-33), el departamento se compromete a mantener una organización efectiva y a colaborar estrechamente con los proveedores de tecnología, asegurando así el éxito y la eficacia del proyecto. Este enfoque establece un modelo de gestión administrativa continuo para el departamento interno de sistemas de la planta.

El proceso de negociación con los proveedores se centra en garantizar la durabilidad de la implementación de los dispositivos. La gestión del desempeño en colaboración con los proveedores es fundamental para supervisar y administrar constantemente los servicios ofrecidos. Esto incluye una serie de pasos destinados a identificar las necesidades en las que el proveedor puede brindar apoyo al departamento.

En ese mismo sentido de mejora se amplía la implementación de bancos de energía robustos de un sistema de alimentación Ininterrumpida (SAI) para mayor cobertura y reforzamiento interno del centro de datos, esto con el motivo de los crecientes cortes de energía, y con base a ello contrarrestar la carga actual del otro banco energético dentro del centro de datos ya existente. Para la instalación se requirió del apoyo de proveedor para el montaje correcto dentro del centro de datos, véase en la referente Figura 34 del antes del montaje, y Figura 35 después del montaje.



Figura 34 Espacio designado al banco de energía interno del centro de datos (ANTES).



Figura 35 Implementación almacén de batería de 8 módulos PX 40KW.



Figura 36 Dispositivos en funcionamiento (cámaras, sensores, y manijas inteligentes).

Fase secundaria instalación de monitor de sala NetBotz 755 en IDF's

Como se mencionó anteriormente en sus especificaciones el NetBotz 755 comprendiendo las características de este, en la Tabla 4 se hace mención de todo un sistema integral de supervisión ambiental y de seguridad creado para asegurar la disponibilidad y protección de entornos, está equipado con diversos sensores que pueden detectar condiciones como la temperatura, la humedad, el flujo de aire, la presión, las vibraciones, la detección de agua, y el monitoreo visual en tiempo real. El mismo dispositivo permite crear interacción entre sensores, y facilita ser integrado dentro de otros sistemas de gestión de infraestructura a niveles holísticos.



Figura 37 IDF-1 Instalación de NetBotz 755 y UPS Vigilancia (surveillance).

En ese mismo sentido de orden se prosiguió la instalación de todos los dispositivos NetBotz 755 que se incorporaron en todos los IDF de la planta (Véase en Figuras 37-45) se genera conexión directa al switch de cada IDF en lo que marca la guía de dirección con el departamento de redes. En conjunto se estipula los mismos lineamientos repetitivos de configuración del NetBotz 750 por medio de configuración por TCP/IP (Véase Tabla 5), Por último, la administración será asumida por el equipo de redes.

Los dispositivos como los UPS utilizados solo se establecieron en un cierto grupo de dispositivos limitados en algunos IDF's, esto consensuado por parte del departamento interno TI así como del departamento de redes (conectividad) priorizando así los dispositivos. Para la funcionalidad de los UPS se conectó una línea que se interconecta directamente al banco de baterías central, cuya conexión en cada UPS va en una línea de 220 V (voltios).

Para los IDF's de las Figuras 37-39 se utilizaron 2 módulos de batería (UPS) como reforzamiento estructural utilizando los modelos SRT5KRMXLT/SRT192BP (Véase Tabla 2). Una vez montado y

coordinando la conexión al switch, se verifica su encendido. En cuanto al departamento de redes hace la instalación del software de gestión del UPS de manera remota, repitiendo mismo proceso en los posteriores IDFs y de la misma forma en la implementación del NetBotz 755, en los otros IDFs.



Figura 39 IDF-2 Instalación de NetBotz 755 y UPS Embarques (shipping).

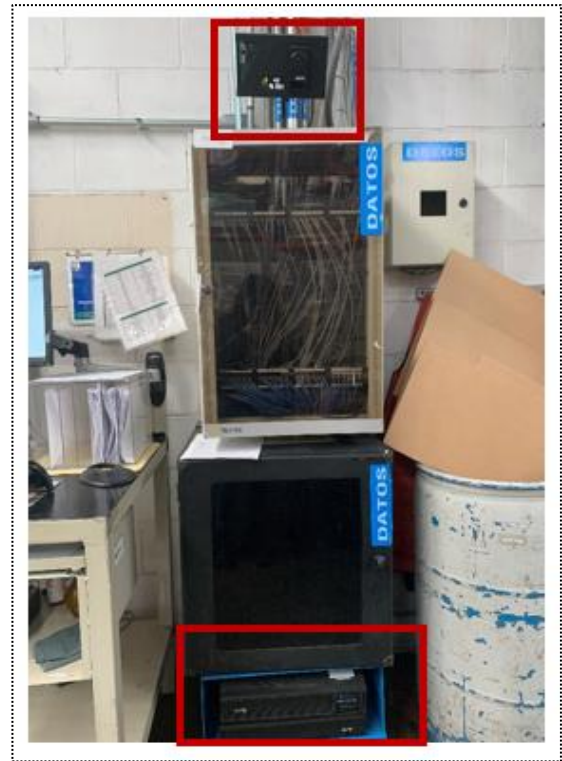


Figura 38 IDF-3 Instalación de NetBotz 755 y UPS Recibo (receiving).

Para el área de embarques en la Figura 38 y Figura 39 se gestionó un gabinete para el sostén de ambos UPS, pidiendo apoyo de proveedor para la elaboración de gabinetes de embarques y recibo, puesto a que forma parte de los requerimientos del sitio, donde se montó un NetBotz 755 en la parte superior, suscitando así la línea que dictan las normatividades sobre la gestión los elementos tecnológicos.

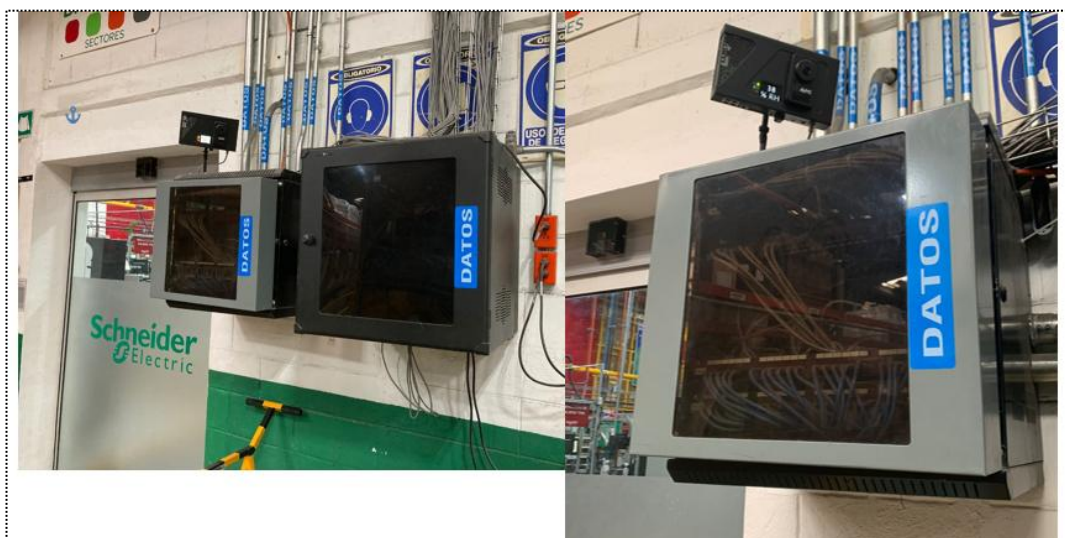


Figura 40 IDF-4 Instalación de NetBotz 755 Pintura (paint).



Figura 41 IDF-5 Instalación de NetBotz 755 y UPS Mantenimiento (Maintenance).



Figura 43 IDF-6 Instalación de NetBotz 755 QOM2 BRK.



Figura 42 IDF-7 Integración de cámara inteligente Mille Auto BRK.

Para ciertos IDFs como se muestran en las Figuras 42-43 se generaron restricciones basadas en las reuniones de despeje, esto influye en la determinación de limitantes, solo se optó por la instalación de NetBotz 755 en QOM2. En el caso de Mille Auto BRK, las condiciones del área limitan el funcionamiento del sistema correcto del NetBotz 755, puesto que el IDF está situado en medio de una línea de producción crítica, por ende, el ambiente que abarca la línea se encuentran otro tipo de sistemas que generan disparos de calor cada vez que un breaker pasa por las validaciones del poka-yoke. Por criterios directivos junto a lado del área de mantenimiento, solo se propuso instalar una cámara inteligente.



Figura 44 IDF-8 Implementación de dispositivos inteligentes Mezzanine BRK.

En la Figura 44 en la parte superior se observa la sala Mezzanine de BRK en dos vistas distintas, por el lado frontal la entrada a la sala, y hacia el fondo se observa el IDF integrado con el banco de baterías modelo G35T30KF4B4S (Véase Tabla 2).

Siendo esta una sala nueva, se instaló el banco de baterías con la asistencia técnica del proveedor verificando así el equipamiento interno de la sala, posterior a ello bajo el criterio del departamento de redes, junto con la administración TI primaria (manage business partner IT), y con la asistencia de soporte interno TI (tech partner) se estableció cumplir con el mismo procedimiento inicial como en el centro de datos (site). Se implementó un NetBotz 750 para montaje en el rack en la parte baja, con el mismo procedimiento de configuración TCP/IP (Véase Tabla 5). Tras esto accede el equipo de redes para hacer las configuraciones necesarias, se mencionó integrar cámaras de monitoreo visual, implementando una cámara visualizando hacia la entrada y una más montada sobre la parte superior

de la entrada, tal cual se observa en la Figura 44 se hizo un cable de red de 5.5 m. que se conectó en la cámara de la entrada subiendo por la parte superior del techo y ocultándose por el plafón cuyo cable también bajo junto a la cámara instalada encima del rack, ocupando así un cable de red de 2 m. donde ambos cables se instalaron bajo el piso de plafón conectándolos directamente al NetBotz. Finalmente, de la misma forma el equipo de redes termino haciendo las configuraciones necesarias para el control de los dispositivos conectados al NetBotz, ahí mismo se instalaron los sensores de temperatura, las chapas inteligentes junto con los imanes para el control de la puerta del rack, integrando con un sensor y expansor de humo modelo NBES0308 (Véase Tabla 2), esta rodea el rack y al mismo tiempo rodea el banco de baterías.

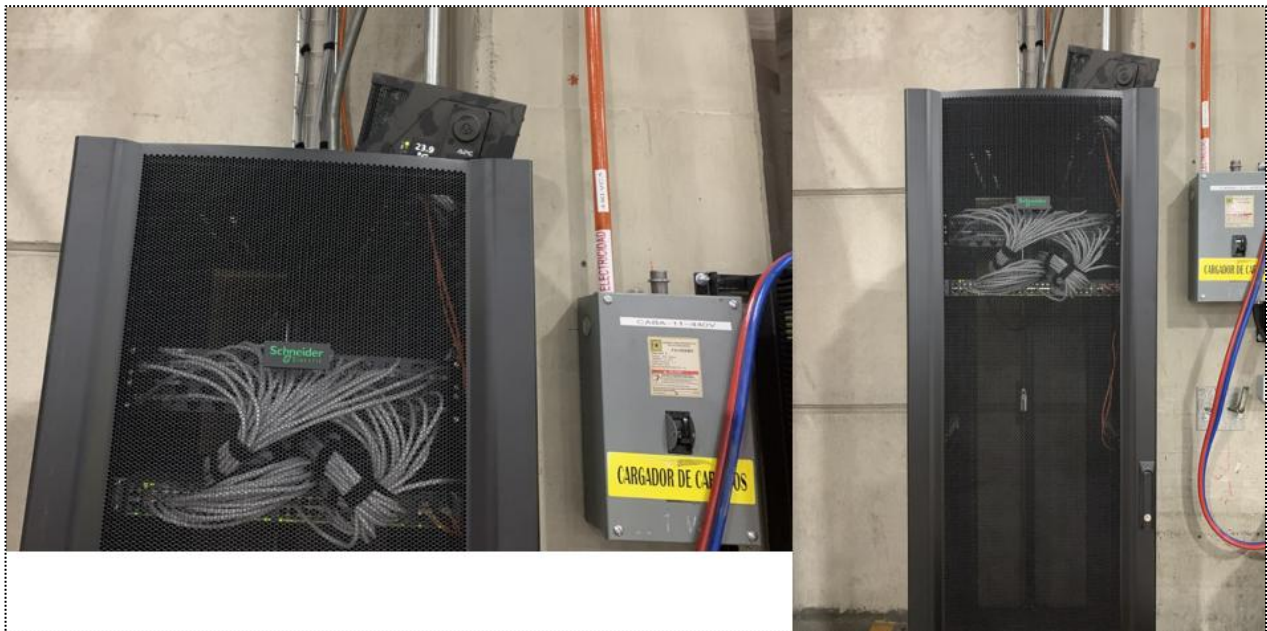


Figura 45 IDF-9 Instalación de NetBotz 755 y rack, Almacén (Warehouse BRK).

Con ayuda de proveedor se estableció restaurar componentes de la infraestructura del IDF observe la Figura 45 reorganizando así los cables y switches de red siendo montado en un rack más sofisticado, de igual forma fue intervenido con la instalación de un NetBotz 755 haciendo de este IDF un modelo resiliente para la infraestructura interna.

IMPACTO Y RESULTADO

Pruebas de funcionalidad y rendimiento

Para enfatizar una vez más este tema, cada uno de los dispositivos montados y conectados en los racks del centro de datos y en los IDF de la planta fue correctamente instalado, esto bajo la supervisión del departamento TI interno de la planta, gerencia TI, y por parte del departamento de redes (conectividad).

La instalación de los dispositivos NetBotz 750 y 755 fue detectado correctamente por el sistema operativo reconoció el hardware sin problemas y sin inconvenientes, todas las pruebas de funcionamiento se realizaron con resultados positivos.

Como se mencionó con anterioridad este proyecto enfoca una gran parte administrativa e integración de la gestión de procesos, esto enfocado y centrado en su parte técnica física, cuyo departamento interno de TI de la planta prioriza la supervisión tangible del funcionamiento de estos dispositivos, una vez instalados, se genera un recorrido de inspección para la verificación del correcto funcionamiento de cada uno de los equipos.

A continuación se muestran algunos sistemas en funcionamiento.



Figura 46 Verificación de funcional banco de baterías del centro de datos.



Figura 47 Verificación funcional del banco de energía en sala (Mezzanine).

Como se muestra en las Figuras 46-47, se verificó que el suministro del banco de baterías este en correcto funcionamiento, proporcionando información detallada sobre el estado del banco. Esta verificación es crucial, ya que se asegura que los sistemas dependientes de esta energía estén siempre operando continuamente. Por medio del manejo del sistema funciona con un software permite mantener los bancos y detectar la carga del suministro eléctrico logrando así emitir alarmas en tiempo real. Estas alarmas son fundamentales para alertar sobre cualquier irregularidad que pudiera surgir en el sistema.

Además, el sistema de baterías puede entrar en un estado de contingencia automáticamente en caso de un corte de energía. Este proceso es automático y esencial, ya que minimiza el tiempo de inactividad y garantiza la continuidad del suministro eléctrico. Cuando se detecta un corte, el sistema activa de inmediato el suministro de rescate eléctrico, el cual es proporcionado por los sistemas de alimentación ininterrumpida (SAI). Estos sistemas de SAIs están diseñados para operar eficazmente, ofreciendo hasta 3 horas de abastecimiento eléctrico, lo que permite tiempo suficiente para estabilizar el sistema o realizar las correcciones necesarias.

Asimismo, este sistema de suministro ininterrumpido se utiliza con la misma intención de garantizar la disponibilidad eléctrica para las conexiones de los IDFs en planta y sus respectivos UPS. Esto es vital, ya que asegura que la infraestructura de red y las comunicaciones permanezcan operativas, incluso ante fallos en el suministro eléctrico espontáneos.



Figura 48 Verificación funcional de UPS.

Haciendo referencia a la Figura 47 finalmente se cierra tema de los sistemas de alimentación ininterrumpida. Al principio del proyecto solo se consideró poco relevante el tema de abarcar suministro eléctrico para equipos de cómputo de líneas críticas de producción que manejan los Andon, (*sistema visual de gestión que se utiliza principalmente en entornos de producción y manufactura*), sin embargo se consideró la integración de UPS para estos equipos, como se observa en la Figura 48, puesto que son de suma importancia, y usualmente se ocupa para la presentación de gráficos de productividad, estos equipos optimizan el trabajo corporativo principalmente para los departamentos de ingeniería como mejora continua, manufactura, calidad, y entre otros. En cada inicio de estas líneas en total se aprobaron 9 UPS, cuyo encendido fue correcto en cada montaje, se instaló el software predeterminado ejecutando así el sistema UPS el cual permite la visualización de gráficos de barras de carga y batería, e incluye alarmas audibles que notifican los cambios en la energía de la red pública y las condiciones de energía del mismo dispositivo UPS.

Retomando una vez más la instalación de los dispositivos NetBotz 750 y 755 fue exitosa y todas las pruebas de funcionamiento se realizaron con resultados positivos durante la instalación y después de. Cuyos segmentos en los dispositivos fueron cubiertos por los aditamentos que se utilizaron para el correcto funcionamiento de estos durante el proceso. Cabe mencionar una vez más, que ambos modelos son dispositivos centralizados y en base a ello estos dispositivos actúan como puntos focales para la coordinación y administración de funciones críticas.

Para esto el departamento interno TI (tech partner) no se le es autorizado en tener acceso a estos sistemas remotos, puesto que la administración queda a cargo del departamento de conectividad (redes).

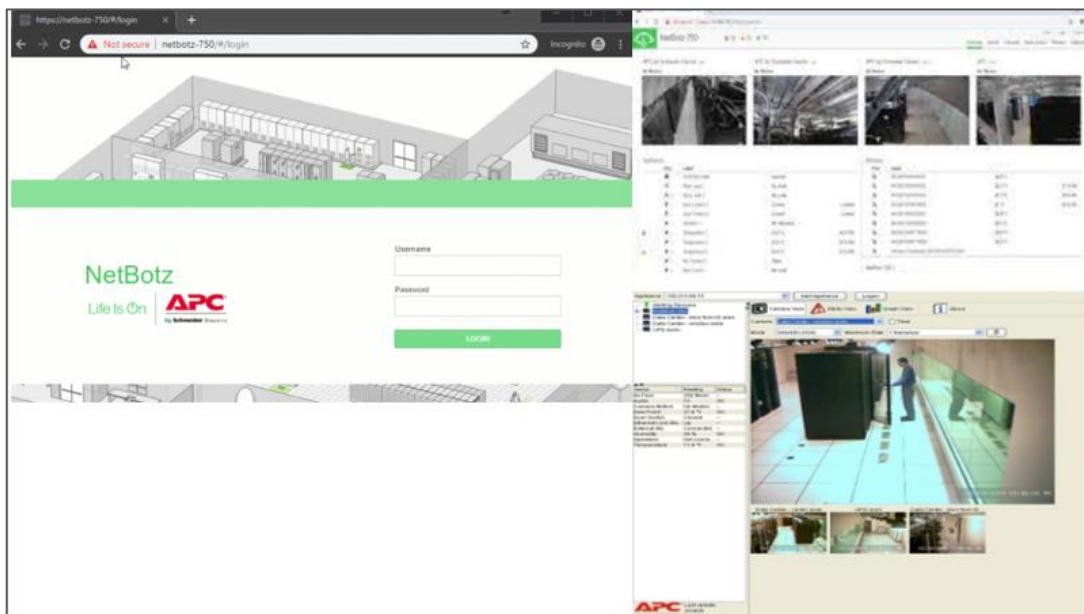


Figura 49 SE Interfaz NetBotz

Nota: La Figura 49 es tomada solo de referencia de Software del dispositivo SE (2019) NetBotz, [imagen digital]. Extraída de <https://www.sE.com/mw/es/product-range/61829-software-para-dispositivos-netbotz-750>.

De esta manera se muestra una interfaz de usuario en tiempo real derivando en un dashboard (tablero de control, herramienta visual que organiza y muestra la información más importante de manera sencilla y fácil de entender, a la visualización de datos, controles /configuración y a la accesibilidad). En palabras cortas esto permite tener y herramientas necesarias para la configuración, monitoreo, y gestión de los datos recopilados.



Figura 50 Verificación funcional del NetBotz 755.

En esta etapa de evaluación general del proceso de instalación se concluyó como eficiente, y completada con éxito. El hardware, se muestra funcionando con alta eficiencia como se muestra en la Figura 50, como referente al cumplimiento con todas las expectativas de rendimiento. Las pruebas de rendimiento mostraron resultados dentro de los parámetros esperados. De acuerdo con eso, todos los criterios de aceptación fueron cumplidos satisfactoriamente y aprobados por la gerencia TI regional, el departamento de conectividad (redes) y, por último, por el departamento interno de TI de la planta.

Mejoras en la resiliencia

Una de las sugerencias para futuras implementaciones se recomienda realizar una verificación inicial exhaustiva del hardware antes de su instalación física. Esto con el fin de verificar la condición del dispositivo, en otros aspectos todos dispositivos actualmente son escalables puesto a que sus componentes tecnológicos cubren una gran variedad de necesidades y pueden ser totalmente resilientes, pero se recomienda que ciertos dispositivos se dispongan del mismo alcance que los actuales, para que puedan generar una conexión íntegra con respecto al resto de los dispositivos.

A continuación, se mencionan algunos criterios del hardware que permiten la comprensión de mejoras en la resiliencia en la infraestructura.

- La redundancia: es totalmente viable porque permite la Integración de múltiples dispositivos en los NetBotz permite redundancia en el monitoreo, y esto garantiza que si un dispositivo falla, otros pueden continuar operando, proporcionando cobertura.
- Automatización y análisis: Los datos recopilados se pueden analizar, esto permite identificar tendencias y prever problemas antes de que ocurran, permitiendo una gestión más proactiva.
- Integración con sistemas de gestión: genera eficiencia en compatibilidad con plataformas de gestión de infraestructura (DCIM) para obtener una infraestructura integra.

Todo esto comprende a temas resilientes ya que permite la entrada a la automatización constante, y si se generase la integración futura de más dispositivos permitirá adaptarse al cambio, cada dispositivo está estimado a cubrir una cobertura de comunicación mucho mayor de 10 años, la actualización de cada dispositivo comprende a mejorar su integración permitiendo así el fácil acceso a la disponibilidad.

Conclusiones

La resiliencia en la infraestructura es esencial hoy en día para garantizar la continuidad de las operaciones y la protección de activos críticos en entornos de las Tecnologías de la Información TI, tal así como hablar de la resiliencia operacional que al final contribuye a la continuidad del negocio que es una de las soluciones para mantener los servicios operando de forma eficiente en caso de estrés o interrupción. En este sentido, la instalación de dispositivos de monitoreo como el NetBotz 750 y NetBotz 755, y aditamentos instalados en los armarios de distribución Intermedia IDF y en el Centro de Datos, es una medida clave para reforzar los sistemas, y al mismo tiempo otorgando confiabilidad. Es importante mencionar que después de lo previamente expuesto, se logró acertar en la adaptación de la metodología Ágil (Scrum) en este proyecto, logrando la gestión de la instalación del hardware, puesto que esto ha optimizado la eficacia en la administración y de los servicios físicos a nivel local. Además, la referencia a marcos y estándares de seguridad ha facilitado una comprensión más amplia de lo que implica gestionar todo un recurso y promoviendo una mejor gestión del entorno de TI. Al implementar este tipo de tecnologías se aprende consecutivamente como administrar y trabajar en equipo, complementando a ello, se logró hacer trabajo colaborativo con proveedores y círculos de ingeniería, esto impulsa a identificar y ampliar el panorama de ideas y soluciones prácticas en sitios estratégicos para el monitoreo y control de accesos obteniendo de esto un equilibrio en el entorno más seguro y bien gestionado. La definición e implementación de sistemas de alimentación ininterrumpida (SAI/UPS) ha reforzado la capacidad de respuesta ante interrupciones, minimizando el impacto en las operaciones.

En conjunto, estos esfuerzos han subrayado la importancia de la resiliencia dentro de la infraestructura TI, destacando su impacto positivo en la estabilidad y eficiencia de los servicios, y sentando las bases para una gestión continua y proactiva de los recursos tecnológicos de la empresa.

La tecnología ofrece una mirada integra de innovaciones y el implementar una resiliencia es dar soluciones de todo tipo. En este proyecto se pudo conocer esos detalles deficientes que generaban ese descontrol por parte del departamento interno TI que eran un problema a nivel planta. Actualmente todo tipo de industria deber ser cubierto por sistemas sólidos, la búsqueda de adaptarse a nuevos medios implica apoyarse en sistemas escalables y automatizados.

Este proyecto finalmente se inclina ante la resiliencia en hardware y aunque el tema implique a tratar con más aspectos no deja de ser un indicativo de generar la confianza empresarial, que conlleva a mejorar las políticas de seguridad. Este resumen resalta cómo los dispositivos NetBotz 750 y 755 son fundamentales para mejorar la resiliencia de la infraestructura en contextos tecnológicos, contribuyendo a proteger, gestionar y mantener eficientemente la continuidad de sistemas críticos, gracias a la integración de los aditamentos que permitieron cubrir las necesidades que demanda la infraestructura de la planta.

Referencias

1. American Psychological Association (2011b, julio 26). Camino a la resiliencia. <https://www.apa.org/topics/resilience/camino>
2. Avendaño, J. (2024, 7 febrero). Qué son los servicios tecnológicos - Centelle. Centelle. <https://www.centelle.mx/blog/que-son-los-servicios-tecnologicos/>
3. Ekon, E. (2023, 12 mayo). Cómo analizar y gestionar el riesgo tecnológico empresarial. Ekon. <https://www.ekon.es/blog/riesgo-tecnologico-empresarial/>
4. Equipo editorial de IONOS. (2023, 12 septiembre). Modelo en espiral: el modelo para la gestión de riesgos en el desarrollo de software. IONOS Startup Guide. <https://www.ionos.mx/startupguide/productividad/modelo-en-espiral/>
5. FIRESMITH, D. (2019, 25 de noviembre). System Resilience: What Exactly is it? Carnegie Mellon University. <https://insights.sei.cmu.edu/blog/system-resilience-what-exactly-is-it/>
6. Gustavsen, A. (n.d.). What is Information Security? Why it's Important, Job Outlook and More. SNHU.edu. Retrieved May 18, 2024, from <https://www.snhu.edu/about-us/newsroom/stem/what-is-information-security>
7. Janco Associates Inc (2017, 09 enero). Technology Resilience and Business Continuity. Available: <https://e-janco.com/articles/2017/2017-01-09-technology-resilience.html>
8. Latam, S. (2023, 28 septiembre). Metodologías Ágiles: qué son y cómo pueden ayudarte. Salesforce. <https://www.salesforce.com/mx/blog/que-son-metodologias-agiles/>
9. Lefort, A. (2019, 02 octubre). La importancia de un DRP (Disaster Recovery Plan). www.teamnet.com.mx. <https://www.teamnet.com.mx/blog/drp-disaster-recovery-plan>
10. Mendoza, M. Á. (2015, 29 de diciembre). Cómo aplicar la resiliencia operativa en infraestructura crítica | WeLiveSecurity. WeLiveSecurity. <https://www.welivesecurity.com/laes/2015/12/29/resiliencia-operativa-infraestructura-critica/>
11. NetBotzTM | APC USA. (s. f.). <https://www.apc.com/us/en/product-range/61830-netbotz/?parentsubcategory-id=88962>
12. Nava, P., & Nava, P. (2023, 30 octubre). Falta de preparación en Arquitectura Tecnológica. Linnoit. <https://linnoit.com/falta-de-preparacion-en-arquitectura-tecnologica/>
13. Página | 73 UPS Industriales | Schneider Electric México. (s. f.). <https://www.se.com/mx/es/product-category/8000-ups-industriales>
14. Paul Kirvan, (2015, agosto) [Online] How do I make a case for a business disaster recovery plan? Available: <https://www.techtarget.com/contributor/Paul-Kirvan/2015>.
15. Prepared by UIT Network Services (July 27, 2018) | UNIVERSITY OF HOUSTON: NETWORK INFRASTRUCTURE STANDARDS, Version 1.25 https://uh.edu/infotech/services/computing/networks/network-infra-standards/network-standards-files/uhnetworkinfrastructurestandards_v01_25.pdf
16. Resilient & Energy-Efficient hardware. (s. f.). Edge Computing Lab. <https://edge.seas.harvard.edu/resilient-and-energy-efficient-hardware>
17. Schneider Electric. (s. f.). APC by Schneider Electric's Education IT Solutions. <https://www.apc.com/us/en/solutions/government-and-education/education/>

18. Stanleigh, M. (2011, 13 de marzo). Risk Management...the What, Why, and How. Business Improvement Architects. <https://bia.ca/risk-management-the-what-why-and-how/>
19. The Most Common Business Continuity and Disaster Recovery Mistakes (Febrero, 2017) [Online]. Available: <https://stonefly.com/blog/common-business-continuity-disasterrecovery-mistakes>
20. Tablado, F. (2021, 13 octubre). Seguridad de hardware para ordenadores de empresa. Grupo Atico34. <https://protecciondatos-lopd.com/empresas/seguridad-hardware/>
21. ¿Qué es la gestión de riesgo de TI? - Guía definitiva. (2021, 24 junio). Acronis. <https://www.acronis.com/es-mx/blog/posts/it-riskmanagement/#:~:text=Qu%C3%A9%20es%20un%20riesgo%20de,TI%2C%20las%20aplicaciones%20y%20datos.>
22. Zola, A. (2022, 11 julio). Intermediate distribution frame (IDF). WhatIs. <https://www.techtarget.com/whatis/definition/intermediate-distribution-frame-IDF>