



Universidad Nacional del Nordeste

Facultad de Ciencias Exactas y Naturales y Agrimensura

“Trabajo Final de Maestría en Tecnologías de la Información”

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco”

Autor: Lic. Alejandro Javier, Alfonso Saucedo

Director: Dr. Horacio Kuna

Año 2022

Dedicatoria

Quiero dedicar humildemente este trabajo, primero a Dios fuente de sabiduría, quien me bendijo con la posibilidad de cursar el posgrado, y llegar a finalizar el mismo.

En segundo lugar, a mi esposa Noelia, quien siempre me apoyó en este desafío de realizar la maestría que anhelaba.

Y finalmente a mis padres quienes siempre estuvieron presentes, y me brindaron una educación de calidad.

Resumen

Este trabajo final de maestría propone la elaboración de un procedimiento para la implementación de Salas Tecnológicas Seguras - STS en el marco de un Sistema de Cableado Estructurado - SCE, basado en los estándares ANSI/TIA 568, 569 y 942, aplicable a cualquier organismo público; contempla la aplicación de las Políticas de Seguridad de la Información - PSI que permiten normar la protección física y del entorno de las STS.

La propuesta surge con el fin de mitigar los riesgos asociados a la seguridad física y ambiental de los dispositivos de ruteo y conmutación de la red de datos de los organismos públicos, y en particular del edificio de Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco.

El enfoque cualitativo del trabajo, nos permitió observar las realidades de los diferentes organismos públicos contemplados en el caso de estudio, e inducir que los más retrasados en pasar de trámites en formato papel a formato electrónico, distan de tener una eficiente infraestructura tecnológica y conectividad, que soporte los nuevos procesos de transformación digital.

La contribución principal del trabajo es el aporte normativo para la gobernanza de las telecomunicaciones en los organismos de la administración pública de la provincia.

Palabras claves: *Salas Tecnológicas Seguras, Sistema de Cableado Estructurado, estándares ANSI/TIA, Seguridad de la Información.*

Abstract

This final master's thesis proposes the development of a procedure for the implementation of Safe Technology Rooms - STS within the framework of a Structured Cabling System - SCE, based on the ANSI / TIA 568, 569 and 942 standards, applicable to any organization; It contemplates the application of the Information Security Policies - PSI that allows to regulate the physical and environmental protection of the STS.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

The proposal arises in order to mitigate the risks associated with the physical and environmental security of the routing and switching devices of the data network of public organizations, and in particular of the building of the Government House of the Executive Power of the Province of Chaco.

The qualitative approach of the work, allowed us to observe the realities of the different public organisms contemplated in the case study, and to induce that those most delayed in moving from procedures in paper format to electronic format, are far from having an efficient technological infrastructure and connectivity, that supports the new processes of digital transformation.

The main contribution of the work is the regulatory contribution for the governance of telecommunications in the public administration agencies of the province.

Keywords: *Secure Technology Rooms, Structured Cabling System, ANSI/TIA standards, Information Security.*

Reconocimiento

Agradezco a mi Director, Dr. Horacio Kuna, por el tiempo brindado y apoyo, por guiarme a lo largo de todo el proyecto del Trabajo Final de Maestría en Tecnologías de Información.

También agradezco a la Secretaría General de Posgrado, Magíster Gladys Noemí Dapozo, quien siempre estuvo presente para responder inquietudes relacionadas a las formalidades de presentación.

Un especial agradecimiento al Arq. Rafael Franco quien hizo docencia conmigo, plasmando sus saberes para concretar un diseño de Sala Tecnológica Segura, que pueda ser aplicado a cualquier organismo.

También al Ing. Civil Alejandro Valussi y al Ing. Electromecánico Ruffino Iturriaga por disponer sus conocimientos en el análisis de especificaciones técnicas para las STS.

Agradezco a mis autoridades superiores, Subsecretaria de Modernización del Estado Tec. Mariela Dolce, y Directora General de Tecnologías de Información y Comunicación Ing. Clarisa Soto, por la confianza depositada en mi persona, de disponer de la libertad para proponer dicho trabajo y poder aplicarlo.

Finalmente, un reconocimiento a todos mis compañeros de trabajo diario, Mariano Avalos y Alejandra Wrobel, entre otros; al personal técnico de ECOM CHACO S.A. Pedro Campestrini, Diego Aguilera, entre otros, quienes fueron parte de éste camino.

Índice

Dedicatoria	II
Resumen	III
Abstract	III
Reconocimiento.....	V
Índice	VI
Figuras.....	VIII
Tablas.....	X
Gráficos.....	XI
Glosario de Términos.....	XII
Capítulo 1.....	15
Introducción	16
1.1 Justificación	16
1.2 Estructura del trabajo final de maestría	17
Capítulo 2.....	21
Marco Teórico.....	22
2.1 Organizaciones de estandarización.....	22
2.2 Estándares de cableado de telecomunicaciones	25
2.3 Estándar ANSI/TIA-568.....	25
2.4 Estándar ANSI/TIA-569.....	30
2.5 Estándar ANSI/TIA-942.....	32
2.6 Políticas de Seguridad de la Información	33
2.7 Antecedentes del tema	37
Capítulo 3.....	41
Descripción de la problemática	42
3.1 Área de conocimiento	43
3.2 Objetivos del Trabajo	44
3.3 Diagnóstico de la situación actual.....	44
3.4 Alcances y limitaciones	47

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

3.5 Metodología	47
Capítulo 4.....	51
Propuesta de solución técnica.....	52
4.1 Salas Tecnológicas Seguras	52
4.2 Sistema de Cableado Estructurado	70
Capítulo 5.....	77
Procedimiento para la implementación de Salas Tecnológicas Seguras (STS).....	78
5.1 Consideraciones Generales	78
5.2 Componentes del procedimiento	81
Capítulo 6.....	89
Evaluación de la propuesta	90
6.1 Descripción del caso de estudio.....	90
6.2 Estimación de riesgos	92
6.3 Discusión de resultados.....	98
Capítulo 7.....	109
Conclusiones y futuras líneas de trabajo.....	110
7.1 Contribuciones del trabajo.....	111
7.2 Futuras líneas de trabajo.....	113
7.3 Avances del proyecto	113
Referencias	115
Anexos	123
Anexo I: Formulario de relevamiento de infraestructura tecnológica.....	124
Anexo II: Instructivo para formulario relevamiento de infraestructura tecnológica.....	128
Anexo III: Informe de Infraestructura Tecnológica 5º Piso Casa de Gobierno.....	137
Anexo IV: Políticas de Seguridad de la Información aplicables a las STS	141
Anexo V: Planos con especificaciones de STS	160
Anexo VI: Riesgos de la Infraestructura Tecnológica de Casa de Gobierno.....	165

Figuras

Figura 1: RJ-45 TIA-568A [15]	26
Figura 2: RJ-45 TIA-568B [17]	26
Figura 3: Relación entre estándares TIA relevantes [1]	28
Figura 4: Subsistemas de Cableado Estructurado [23].....	30
Figura 5: Principios Rectores Ley 3203-A [Elaboración propia]	45
Figura 6: Ejes Principales del CTD [Elaboración propia]	46
Figura 7: Enfoque cualitativo del fenómeno en estudio [Elaboración propia]	48
Figura 8: Topología 1 [Elaboración propia]	60
Figura 9: Topología 2 [Elaboración propia]	61
Figura 10: Topología 3 [Elaboración propia]	61
Figura 11: Organización de rack principal [Elaboración propia]	65
Figura 12: Planta General - Corte [Elaboración propia]	66
Figura 13: Corte - Cielorraso [Elaboración propia].....	66
Figura 14: Vista interna de STS [Elaboración propia]	67
Figura 15: Vista externa de STS [Elaboración propia]	68
Figura 16: Vista de STS ampliada [Elaboración propia].....	68
Figura 17: Vista lateral con corte de STS [Elaboración propia]	69
Figura 18: Vista superior de canalización de STS [Elaboración propia].....	69
Figura 19: Vista superior inclinada de canalización de STS [Elaboración propia]	70
Figura 20: Distancias máximas para el cableado horizontal [49]	72
Figura 21: MUTO [50]	72
Figura 22: Punto de consolidación [50]	73
Figura 23: Secuencia de componentes del procedimiento [Elaboración propia]	81
Figura 24: DFP del Informe de Infraestructura Tecnológica [Elaboración propia]	82
Figura 25: DFP de la Obra Civil de la STS [Elaboración propia]	83
Figura 26: DFP de la adquisición de electrónica y elementos de conectividad para la STS [Elaboración propia]	84
Figura 27: STS en Casa de Gobierno [Elaboración propia]	90
Figura 28: Diseño físico red de datos Casa de Gobierno [Elaboración propia].....	91

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Figura 29: Metas intermedias 43, 44 y 45 -SIGOB [54] 112

Figura 30: Meta intermedia 40 - SIGOB [55] 113

Tablas

Tabla 1: Subsistemas del estándar ANSI/TIA 942 [24]	33
Tabla 2: Obra civil STS [Elaboración propia]	62
Tabla 3: Electrónica y elementos de conectividad [Elaboración propia]	63
Tabla 4: Distancias máximas admisibles con un dispositivo MUTO [50]	73
Tabla 5: Elementos del cableado horizontal [Elaboración propia]	74
Tabla 6: Secciones del formulario de relevamiento [Elaboración propia]	80
Tabla 7: Riesgos de la infraestructura tecnológica [Elaboración propia]	80
Tabla 8: Escalas cualitativas [3]	92
Tabla 9: Estimación del riesgo [3]	92
Tabla 10: Datos relevados 5° piso Casa de Gobierno [Elaboración propia]	92
Tabla 11: Riesgo servidores sin respaldo de datos [Elaboración propia]	94
Tabla 12: Riesgo los servidores no cuentan con UPS [Elaboración propia]	95
Tabla 13: Riesgo espacio físico no delimitado [Elaboración propia]	95
Tabla 14: Riesgo conexiones eléctricas deficientes [Elaboración propia]	96
Tabla 15: Riesgo cableado de red no documentado [Elaboración propia]	96
Tabla 16: Riesgo red no administrada [Elaboración propia]	97
Tabla 17: Resultado de la estimación de riesgos 5º Piso [Elaboración propia]	97
Tabla 18: Resultados Informe IT por piso del edificio [Elaboración propia]	98
Tabla 19: Estimaciones de riesgos por piso [Elaboración propia]	100
Tabla 20: Salvaguardas por riesgo [Elaboración propia]	104
Tabla 21: Estimación de costos STS [Elaboración propia]	106
Tabla 22: Estimación para 4000 puestos de red [Elaboración propia]	107
Tabla 23: Estimación para 12 STS [Elaboración propia]	107
Tabla 24: Estimación total de costos para el proyecto [Elaboración propia]	108

Gráficos

Gráfico 1: Resultado Informes IT del edificio	100
Gráfico 2: Riesgo servidores sin respaldo de datos.....	101
Gráfico 3: Riesgo los servidores no cuentan con una protección energética (UPS)	101
Gráfico 4: Riesgo espacio físico no delimitado.....	102
Gráfico 5: Riesgo conexiones eléctricas deficientes.....	102
Gráfico 6: Riesgo cableado de red no documentado	103
Gráfico 7: Riesgo red no administrada	103

Glosario de Términos

TIC: Tecnología de Información y Comunicación.

STS: Sala Tecnológica Segura.

SCE: Sistema de Cableado Estructurado.

PSI: Políticas de Seguridad de la Información.

CTD: Consejo Provincial de Transformación Digital.

CCIA: Computer Communications Industry Association -
Asociación de la Industria de las Comunicaciones Informáticas.

ISO: International Organization for Standardization - Organización Internacional para la Estandarización.

IEC: International Electrotechnical Commission – Comisión Electrotécnica Internacional.

ANSI: American National Standards Institute - Instituto Americano Nacional de Estándares.

TIA: Telecommunications Industry Association - Asociación de Industrias de Telecomunicaciones.

EIA: Electronic Industries Alliance - Alianza de Industrias Electrónicas.

ECA: Electronic Components, Assemblies and Materials Association - Asociación de componentes, ensamblajes y materiales electrónicos.

NEDA: National Electronic Distributors Association - Asociación Nacional de Distribuidores Electrónicos.

ECIA: Electronic Components Industry Association - Asociación de la Industria de Componentes Electrónicos.

IEEE: Institute of Electrical and Electronic Engineers - Instituto de Ingenieros Eléctricos y Electrónicos.

CENELEC: European Committee for Electro technical Standardization - Comité Europeo para la Estandarización Electrotécnica.

TR-42: Telecommunications Cabling Systems - Sistemas de Cableado de Telecomunicaciones.

COPANT: Comisión Panamericana de Normas Técnicas.

AMN: Asociación Mercosur de Normalización.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

ONN: Organismos Nacionales de Normalización.

GMC: Grupo Mercado Común.

AEA: Asociación Electrotécnica Argentina.

INTI: Instituto Nacional de Tecnología Industrial.

UTP: Unshielded twisted pair - cable de par trenzado sin blindaje.

NVR: Network video recorder - Grabador de video en red.

UPS: Uninterruptable Power Supply - Fuente de alimentación ininterrumpida.

DGTIC: Dirección General de Tecnologías de Información y Comunicación.

MAJ: Máxima Autoridad Jurisdiccional.

MPEI: Ministerio de Planificación, Economía e Infraestructura.

SPP: Subsecretaría de Planificación y Proyectos de Obras.

DP: Dirección de Proyectos.

DGTIC: Dirección General de Tecnologías de la Información y Comunicación

ECOM: Empresa Ecom Chaco S.A.

JUR: Refiere a la jurisdicción u organismo donde se implementará la Sala Tecnológica Segura.

STS: Sala Tecnológica Segura.

PEF: Propuesta de Espacio Físico.

PEO: Proyecto Ejecutivo de Obra.

RI: Responsable Informático.

DFP: Diagrama de Flujo del Procedimiento.

BID: Banco Interamericano de Desarrollo.

FGS: Fondo de Garantía de Sustentabilidad.

SIGOB: Sistema de Gestión para la Gobernabilidad.

PNUD: Programa de Naciones Unidas para el Desarrollo.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Capítulo 1

Introducción

Introducción

El presente trabajo surge como respuesta a la necesidad de mitigar los riesgos asociados a la seguridad física y ambiental de los dispositivos de ruteo y conmutación de las redes de datos de los organismos públicos, tomando como caso de estudio el edificio de Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco.

La propuesta se basa en elaborar un procedimiento para la implementación de Salas Tecnológicas Seguras (STS) en organismos públicos en el marco de un Sistema de Cableado Estructurado (SCE), para alojar los equipos y recursos de conectividad que conforman los troncales o backbone de los edificios públicos.

Previamente a la redacción del procedimiento, se plasman las especificaciones para las STS, los criterios y lineamientos para un SCE, analizando los estándares de la industria que norman lo referido a telecomunicaciones.

Finalmente, para la evaluación del procedimiento se estiman los riesgos de seguridad física y ambiental aplicables a la infraestructura tecnológica de los organismos del caso de estudio.

1.1 Justificación

Las normas y estándares de telecomunicaciones se diseñaron con el objetivo de fijar especificaciones para equipos, elementos y materiales de conectividad, facilitando la compatibilidad de productos entre fabricantes. La aplicación de éstas, debe establecer prácticas apropiadas de seguridad y determinar la aplicabilidad de las mismas, teniendo en cuenta limitaciones antes de su uso, así como las normativas regulatorias gubernamentales.

El estándar de referencia del cableado genérico de telecomunicaciones para las instalaciones del cliente, es la norma ANSI/TIA 568.0-E [1], la cual se relaciona con otros estándares desarrollados por la Asociación de la Industria de las Telecomunicaciones (TIA) [2]. La aplicación de dicha norma, muchas veces se ve obstaculizada por las exigencias propias del estándar, lo que repercute en altos costos de implementación. Es por ello que se decidió tomar de dicho estándar y los relacionados al mismo, características para ser aplicados a un

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

modelo de Sala Tecnológica Segura (STS), que pueda ser implementado en los organismos públicos del Poder Ejecutivo de la Provincia del Chaco.

Lo mencionado en el párrafo anterior se debe, a que generalmente se encuentran en una misma sala o cuarto, los recursos informáticos que deberían estar en la sala de equipos o en la sala de telecomunicaciones. Es por ello que la propuesta de las Salas Tecnológicas Seguras (STS), incorpora características edilicias priorizando la seguridad física y ambiental, para que puedan contener equipamiento y electrónica de ambas salas o cuartos.

1.2 Estructura del trabajo final de maestría

El contenido del trabajo final de maestría se visualiza en 7 capítulos, sus referencias y 6 anexos, que se detallan a continuación:

Capítulo 1. Introducción

En ésta sección se plasma la necesidad que motiva el presente trabajo final de maestría, de elaborar un "Procedimiento para la implementación de Salas Tecnológicas Seguras (STS) en organismos públicos en el marco de un Sistema de Cableado Estructurado (SCE)". Luego su justificación se basa en la adaptación de los estándares al caso de aplicación, para finalizar con el propósito propuesto.

Capítulo 2. Marco Teórico

El Marco Teórico aborda el estudio de las organizaciones de estandarización y normas de la industria referidas a telecomunicaciones, como también las normativas internacionales, nacionales y provinciales, relacionadas con la seguridad física y ambiental de las políticas de seguridad de la información que son aplicables a las STS.

Capítulo 3. Descripción del problema

El problema se describe en función de la necesidad de adaptar los estándares de referencia en materia de telecomunicaciones al caso de estudio, priorizando la seguridad física y ambiental de la infraestructura de telecomunicaciones de los organismos. Así mismo, se plasma el área de conocimiento en el cual se enmarca el trabajo, los objetivos, un diagnóstico actual, su alcance, limitaciones y metodología de investigación utilizada.

Capítulo 4. Propuesta de solución técnica

La propuesta de solución técnica se basa en la aplicación de los estándares ANSI/TIA 568, 569 y 942. La sección plasma las especificaciones para las Salas Tecnológicas Seguras (STS), así como los criterios y lineamientos que se deben aplicar en un Sistema de Cableado Estructurado (SCE).

Capítulo 5. Procedimiento para la implementación de STS dentro de un SCE

El procedimiento parte de un relevamiento de la infraestructura tecnológica de los organismos públicos, mediante un formulario de relevamiento con su correspondiente instructivo, y en base a una estimación de riesgos de los datos relevados, plasma un informe positivo o negativo, que expone si el organismo amerita o no la implementación de una STS, para mitigar los riesgos que pueden afectar la seguridad física y ambiental de las STS.

Capítulo 6. Evaluación de la propuesta

La evaluación de la propuesta, se basa en una estimación de riesgos de los datos relevados, aplicando un análisis mediante tablas, como lo describe el Libro Guía de Técnicas de Magerit V3 [3]. La observación hace foco en las salvaguardas aplicadas a los riesgos que pueden afectar la seguridad física y ambiental de la infraestructura tecnológica de los organismos públicos. El resultado obtenido, se plasma en un informe de la infraestructura tecnológica, que, de acuerdo a los fundamentos expuestos en el mismo, aprobará o no la petición formal de la construcción de STS en el organismo.

Capítulo 7. Conclusiones y futuras líneas de trabajo

En este capítulo se presentan las conclusiones finales del trabajo final de maestría, además de las contribuciones del mismo para avanzar en la gobernanza de la infraestructura tecnológica en la provincia. También se plantean líneas de trabajo futuro, como trabajar en un procedimiento de auditoría de las STS que se implementen.

Referencias

En ésta sección se visualiza la bibliografía de referencia utilizada en el trabajo desarrollado.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Anexos

Finalmente, en ésta sección se presentan seis anexos, constituidos por Anexo I: Formulario de relevamiento de infraestructura tecnológica, Anexo II: Instructivo para formulario relevamiento de infraestructura tecnológica, Anexo III: Informe de Infraestructura Tecnológica 5º Piso Casa de Gobierno, Anexo IV: Políticas de Seguridad de la Información aplicables a las STS, Anexo V: Planos con especificaciones de STS, y Anexo VI: Riesgos de la Infraestructura Tecnológica de Casa de Gobierno.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Capítulo 2

Marco Teórico

Marco Teórico

En este capítulo se presenta el estudio de las organizaciones de estandarización y normas de la industria referidas a telecomunicaciones, como también las normativas internacionales, nacionales y provinciales, relacionadas a la seguridad física y ambiental de las políticas de seguridad de la información que son aplicables a las STS. También se describen las revisiones y principales características de los estándares ANSI/TIA 568, ANSI/TIA 569 y ANSI/TIA 942. El capítulo finaliza con antecedentes del tema planteado, haciendo referencia a otros trabajos que abordan la aplicación de estos estándares.

2.1 Organizaciones de estandarización

Actualmente en el mundo, hay una gran diversidad de organizaciones involucradas en la elaboración de normas y estándares. Entre las más relevantes se encuentran:

ISO (International Organization for Standardization - Organización Internacional para la Estandarización) [4].

Es una organización independiente y no-gubernamental, formado por las organizaciones de normalización de 164 países miembros, con una oficina central en Ginebra, Suiza, que coordina el sistema y publica las normas, además de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales, a excepción de la eléctrica y la electrónica.

IEC (International Electro technical Commission – Comisión Electrotécnica Internacional) [5].

Es una organización casi gubernamental sin fines de lucro, fundada en 1906, y en la cual sus miembros son Comités Nacionales que designan a expertos, y delegados provenientes de la industria, organismos gubernamentales, academia y asociaciones, para participar en el trabajo de evaluación técnica y de conformidad de la IEC.

Es líder mundial en la preparación y publicación de Normas Internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas, que se conocen colectivamente como "electrotecnología", y proporciona una plataforma a empresas, industrias y gobiernos para cumplir, discutir y desarrollar los estándares internacionales que requieren.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

ANSI (American National Standards Institute - Instituto Americano Nacional de Estándares) [6].

Es una organización privada sin fines de lucro, que administra y coordina la normalización voluntaria de los Estados Unidos. Supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. La organización, también coordina estándares del país estadounidense con estándares internacionales, de tal modo que los productos de dicho país puedan usarse en todo el mundo.

TIA (Telecommunications Industry Association - Asociación de Industrias de Telecomunicaciones) [2].

Es una organización de desarrollo de estándares acreditada por ANSI, y la principal organización que representa mundialmente a las industrias de las tecnologías de la información y comunicación (TIC) a través del desarrollo de estándares, normas de cableado industrial y estructurado. Cuenta con la ayuda de más de 500 miembros, comités de ingeniería y organizaciones asociadas en América, Europa-Medio Oriente y Asia-Pacífico.

EIA (Electronic Industries Alliance - Alianza de Industrias Electrónicas).

Fue la principal organización comercial que representaba a la comunidad de alta tecnología de EE. UU. Fundada en 1924 como la Asociación de Fabricantes de Radio.

La Alianza dejó de existir formalmente el 11 de febrero de 2011. La EIA designó a ECA (Electronic Components, Assemblies and Materials Association - Asociación de componentes, ensamblajes y materiales electrónicos) para continuar desarrollando estándares para componentes electrónicos de interconexión y electromecánicos, bajo la designación ANSI de los estándares EIA. La ECA se fusionó con la NEDA (National Electronic Distributors Association - Asociación Nacional de Distribuidores Electrónicos) en 2011, para formar la ECIA (Electronic Components Industry Association - Asociación de la Industria de Componentes Electrónicos) [7].

IEEE (Institute of Electrical and Electronic Engineers - Instituto de Ingenieros Eléctricos y Electrónicos) [8].

Es una asociación dedicada a promover innovación y excelencia tecnológica en beneficio de la humanidad, se considera la sociedad técnica más grande del mundo. IEEE es una empresa líder en el desarrollo de normas internacionales que sustentan muchas de las

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

telecomunicaciones de hoy en día, la tecnología de la información y productos de generación de energía y servicios. A menudo es la fuente central para la normalización en una amplia gama de tecnologías emergentes.

CENELEC (European Committee for Electro technical Standardization - Comité Europeo para la Estandarización Electrotécnica) [9].

Desarrolla los estándares electrotécnicos para la mayor parte de Europa. El CENELEC es una organización técnica sin ánimo de lucro, amparada por la legislación belga y compuesta por comités electrotécnicos nacionales que representan a 28 países europeos.

La misión del CENELEC es preparar normas electrotécnicas de carácter voluntario, que ayude a desarrollar un mercado único europeo para productos, servicios eléctricos y electrónicos, eliminando las barreras comerciales, creando nuevos mercados y reduciendo los costos de adaptación.

IRAM (Instituto Argentino de Normalización y Certificación) [10].

Estudia y publica normas argentinas en todos los campos de actividad, que favorecen y facilitan el desarrollo económico y social, lo cual contribuye a mejorar la calidad de vida y el uso racional de los recursos.

Participa activamente como representante de la República Argentina, en los procesos de normalización internacional, en ISO [4] e IEC [5], y en la normalización regional, en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación Mercosur de Normalización (AMN). IRAM es representante de dichos organismos en nuestro país.

Es reconocido por el Estado como el único organismo de normalización de Argentina, y desarrolla su actividad a través de más de 350 organismos técnicos de estudio de normas, en los que participan representantes de la producción, el consumo, la ciencia y la técnica, la educación y el gobierno.

COPANT (Comisión Panamericana de Normas Técnicas) [11].

En Nueva York, en 1964, la Asamblea General del Comité Panamericano, cambió su denominación a la de Comisión Panamericana de Normas Técnicas, bajo el título abreviado de COPANT. Es un organismo regional de normalización que agrupa a los Organismos Nacionales de Normalización (ONN) de las Américas.

AMN (Asociación Mercosur de Normalización) [12].

La Asociación Mercosur de Normalización, creada en la década de 1990, es el organismo responsable de gestionar la normalización en el ámbito del Mercosur.

Participan de la misma, los Organismos Nacionales de Normalización (ONN) de Argentina, Brasil, Uruguay, Paraguay, Chile y Bolivia (éstos dos últimos como invitados).

2.2 Estándares de cableado de telecomunicaciones

Estándares TIA: Comité TR-42 "Sistemas de cableado de telecomunicaciones" [13]

El Comité de Ingeniería TR-42 de la Asociación de la Industria de las Telecomunicaciones (TIA) [2], está formado por un grupo de empresas e instituciones con roles de liderazgo alternativos. Su atención se centra en las infraestructuras de cableado de telecomunicaciones para edificios residenciales, comerciales, industriales, hogares, centros de datos, etc. Las normas abarcan componentes de cableado, instalación y prueba de la infraestructura de telecomunicaciones de un edificio.

2.3 Estándar ANSI/TIA-568

Esta norma publicada en 1991, constituye el primer estándar para cableado de comunicaciones. El mismo fue desarrollado por el comité de ingeniería TR-42 [13] de la TIA (Asociación de la Industria de las Telecomunicaciones) [2].

Para convertirse en una norma oficial de Estados Unidos, el estándar TIA/EIA-568 fue presentado a la ANSI (Instituto Americano Nacional de Estándares) [6]. A partir de allí se le denominó estándar ANSI/TIA/EIA-568.

Como la EIA (Electronic Industries Alliance - Alianza de Industrias Electrónicas), dejó de existir formalmente el 11 de febrero de 2011, las actualizaciones de los estándares para cableado de comunicaciones se identifican con las organizaciones ANSI/TIA.

2.3.1 Revisiones del estándar ANSI/TIA-568

La **revisión A** fue la primera actualización de la norma, publicada en el año 1995, su nomenclatura es reconocida con las siglas ANSI/TIA/EIA 568-A [14]. La misma define el diseño, construcción y administración de un Sistema de Cableado Estructurado (SCE), plasma

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

requerimientos mínimos para el cableado de oficinas de edificios comerciales, y hace recomendaciones para la topología de la red, las distancias máximas de los cables, así como el rendimiento de los componentes.

Esta norma admite el uso de cable UTP categoría 5, y también define un código de colores para los conectores RJ45, como se muestra en la Figura 1.

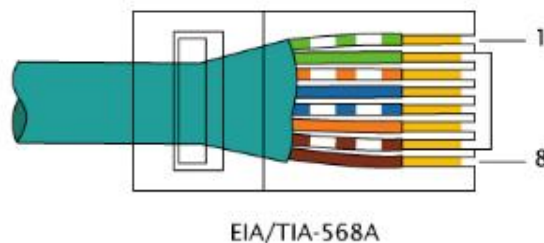


Figura 1: RJ-45 TIA-568A [15]

La **revisión B** es la segunda actualización de la norma, publicada en el año 2001, su nomenclatura es reconocida con las siglas ANSI/TIA/EIA 568-B [16]. Esta incorpora el diseño de un SCE para edificios situados en entornos de campus. Si bien admite el uso de cable UTP categoría 5, éste último fue reemplazado por la categoría 5e (enhanced o mejorada) con la cual se puede alcanzar velocidades de hasta 1 Gbps (Gigabit por segundo). La revisión define otro código de colores para los conectores RJ45, como se muestra en la Figura 2.

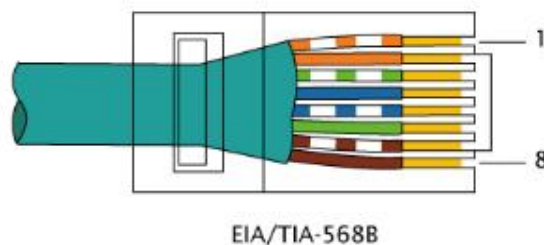


Figura 2: RJ-45 TIA-568B [17]

La **revisión C** es la tercera actualización de la norma, publicada en el año 2009, su nomenclatura es reconocida con las siglas ANSI/TIA 568-C [18], y constituye una nueva generación de estándares de cableado, conformada por una familia de estándares relacionados. Entre los mismos se encuentran:

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

"ANSI/TIA-568-C.0, Cableado genérico de telecomunicaciones para las instalaciones del cliente, publicado en 2009;

ANSI/TIA-568-C.1, Estándar de cableado de telecomunicaciones para edificios comerciales, publicado en 2009;

ANSI/TIA-568-C.2, Estándar de componentes y cableado de telecomunicaciones de par trenzado balanceado, publicado en 2009;

ANSI/TIA-568-C.3, Estándar de componentes de cableado de fibra óptica, publicado en 2008;

ANSI/TIA-568-C.4, Estándar de componentes y cableado coaxial de banda ancha, publicado en 2011" [19].

Esta revisión incluye además de las categorías 5e y 6 para cable UTP, la categoría 6 aumentada (cat. 6A) como tipo de medio reconocido, y reúne las adendas de la versión anterior, permitiendo compilar en un solo documento las mismas. Fue desarrollado como documento genérico para ser utilizado, cuando un estándar específico no estuviera disponible (por ejemplo, para instalaciones de servicios de salud).

La **revisión D** es la cuarta actualización de la norma, publicada en el año 2015, su nomenclatura es reconocida con las siglas ANSI/TIA 568.0-D [20], y algunos de sus cambios significativos son:

"Se requiere cableado UTP de categoría 5e o superior para todas las implementaciones de cableado de par trenzado balanceado genérico. Se ha agregado cableado coaxial de banda ancha como un medio reconocido" [21], entre otros.

La **revisión E** es la última actualización de la norma, publicada en marzo del 2020, su nomenclatura es reconocida con las siglas ANSI/TIA 568.0-E [1], y algunos de sus cambios significativos son:

"Se recomienda implementar dos tendidos de cableado de categoría 6A o superior en cada punto de acceso inalámbrico. Se han agregado como elementos funcionales conectores de punto de conexión horizontal y topologías del subsistema de cableado 1" [22], entre otros.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

2.3.2 Relación con otros estándares ANSI/TIA

La norma ANSI/TIA 568, en su última revisión, se relaciona con otros estándares TIA relevantes de la industria, como se visualiza en la Figura 3.



Figura 3: Relación entre estándares TIA relevantes [1]

Dicha relación agrupa los mismos en tres grupos:

1. Estándares comunes:

- ANSI/TIA-568.0: Cableado genérico de telecomunicaciones para las instalaciones del cliente.
- ANSI/TIA-569: Vías y espacios de telecomunicaciones.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- ANSI/TIA-606: Estándar de administración para infraestructura de telecomunicaciones.
- ANSI/TIA-607: Conexión y puesta a tierra de telecomunicaciones genéricas para las instalaciones del cliente.
- ANSI/TIA-758: Estándar de infraestructura de telecomunicaciones de planta externa propiedad del cliente.
- ANSI/TIA 862: Estándar de infraestructura de cableado estructurado para sistemas de edificios inteligentes.
- ANSI/TIA-4994: Estándar para tecnología de comunicaciones de información sostenible.
- ANSI/TIA-5017: Estándar de seguridad de red física de telecomunicaciones.

2. Estándares de las instalaciones:

- ANSI/TIA-568.1: Estándar de infraestructura de telecomunicaciones de edificios comerciales.
- ANSI/TIA-570: Estándar de telecomunicaciones residencial.
- ANSI/TIA-942: Estándar de infraestructura de telecomunicaciones para centros de datos.
- ANSI/TIA-1005: Estándar de infraestructura de telecomunicaciones para instalaciones industriales.
- ANSI/TIA-1179: Estándar de infraestructura de telecomunicaciones para instalaciones sanitarias.
- ANSI/TIA-4966: Estándar de infraestructura de telecomunicaciones para instalaciones educativas.

3. Estándares de cableado y componentes:

- ANSI/TIA-568.2: Estándar de componentes y cableado de telecomunicaciones de par trenzado balanceado.
- ANSI/TIA-568.3: Estándar de componentes y cableado de fibra óptica.
- ANSI/TIA-568.4: Estándar de componentes y cableado coaxial de banda ancha.

2.4 Estándar ANSI/TIA-569

Esta norma fue publicada en octubre de 1990, y también la redactó el comité de ingeniería TR-42 [13] de la TIA (Asociación de la Industria de las Telecomunicaciones) [2].

2.4.1 Revisiones del estándar ANSI/TIA-569

La **revisión A** fue la primera actualización de la norma, publicada en febrero del año 1998.

La **revisión B** fue la segunda actualización de la norma, publicada en octubre del año 2004.

La **revisión C** fue la tercera actualización de la norma, publicada en mayo del año 2012.

La **revisión D** fue la cuarta actualización de la norma, publicada en abril del año 2015.

La **revisión E** fue la última actualización de la norma, publicada en mayo del año 2019.

2.4.2 Componentes en la infraestructura

El diseño arquitectónico debe contemplar el sistema de cableado de telecomunicaciones, al igual que otros sistemas, como el eléctrico. Es por ello que éste estándar provee especificaciones para la instalación e infraestructura de comunicaciones en edificios, de manera de soportar los requerimientos actuales y futuros de los sistemas de telecomunicaciones. El estándar está compuesto por subsistemas de cableado estructurado, como se visualiza en la Figura 4.

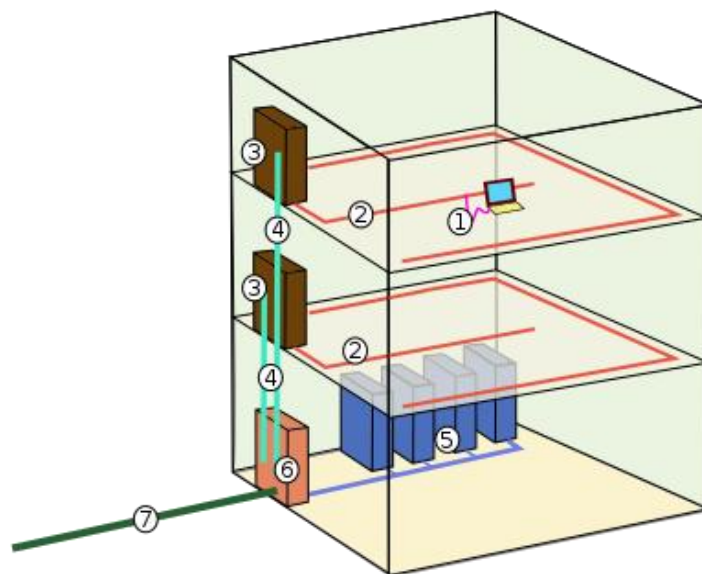


Figura 4: Subsistemas de Cableado Estructurado [23]

1. Áreas de Trabajo

Las áreas de trabajo comprenden los puestos que necesitan bocas de red disponibles, a las cuales pueden conectarse los usuarios desde sus escritorios. Un área de trabajo puede integrar más de un elemento de conexión en el sistema de cableado estructurado.

2. Cableado horizontal

El cableado horizontal contempla las canalizaciones y elementos necesarios para conectar un área de trabajo a la sala o cuarto de telecomunicaciones del piso.

3. Cuarto de Telecomunicaciones

Las salas o cuartos de telecomunicaciones son áreas exclusivas dentro de un edificio, para la electrónica de conectividad de telecomunicaciones. Su función principal es la terminación del cableado horizontal y vertical.

4. Cableado vertical o backbone

El cableado vertical permite interconectar las salas o cuartos de telecomunicaciones, y cuarto de equipos a las instalaciones de entrada del edificio. También incluye el cableado entre edificios.

5. Cuarto de Equipos

La sala o cuarto de equipos está pensada para contener equipos que brindaran comunicación al edificio, como centrales telefónicas y de video, equipos informáticos.

6. Acometida de entrada

La acometida está compuesta por las instalaciones de entrada al edificio, esta comprende a todos los dispositivos de protección, hardware de conexión y cables, que se conectan al cableado del proveedor de servicios. Se suele utilizar como punto de demarcación, para fijar las responsabilidades entre el prestador de servicios y los organismos que utilizan el mismo.

7. Cableado de campus

Es el cableado que conecta los diferentes distribuidores de edificios, con el distribuidor de campus, puede ser tanto fibra óptica, como cable de par trenzado o incluso coaxial. Una característica importante de los troncales de cableado que conforman el sistema de campus

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

es que deben estar preparados para ambientes exteriores: protegidos contra humedad, roedores, etc.

2.5 Estándar ANSI/TIA-942

Esta norma se publicó en abril de 2005, y también la redactó el comité de ingeniería TR-42 [13] de la TIA (Asociación de la Industria de las Telecomunicaciones) [2].

2.5.1 Revisiones del estándar ANSI/TIA-942

En marzo del año 2008 se publicó el **Anexo 1** de la norma, que refiere a las *Especificaciones de cableado coaxial del centro de datos y distancias de aplicación*.

En febrero del año 2010 se publicó el **Anexo 2** de la norma, que plasma *Directrices adicionales para centros de datos*.

En marzo del año 2014 se publicó la **revisión A** de la norma.

En julio del año 2017 se publicó la última **revisión B** de la norma.

2.5.2 Clasificación de centros de datos

El estándar establece las características que deben ejecutarse en los componentes de la infraestructura, para los distintos grados de disponibilidad de los centros de datos. Los niveles más altos corresponden a una mayor solidez del sistema, y también conducen a una mayor inversión en infraestructura.

El estándar proporciona una clasificación de cuatro niveles para los centros de datos:

- El sistema de niveles está destinado a mejorar la confiabilidad y solidez del centro de datos.
- Las calificaciones de nivel 1, 2, 3 y 4 se asignan en cuatro áreas:
 1. Telecomunicaciones
 2. Arquitectura
 3. Eléctrica
 4. Mecánica

Tabla 1: Subsistemas del estándar ANSI/TIA 942 [24]

Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
Cableado de racks	Selección del sitio	Cantidad de accesos	Sistemas de climatización
Accesos redundantes	Tipo de construcción	Puntos únicos de falla	Presión positiva
Cuarto de entrada	Protección ignífuga	Cargas críticas	Cañerías y drenajes
Área de distribución	Requerimientos NFPA 75 (Sistemas de protección contra el fuego para información)	Redundancia de UPS	Chillers (Enfriadores)
Backbone	Barrera de vapor	Topología de UPS	CRAC's y condensadores
Cableado horizontal	Techos y pisos	PDU's (Unidades de distribución de energía)	Control de HVAC (Aire acondicionado de alta ventilación)
Elementos activos redundantes	Área de oficinas	Puesta a tierra	Detección de incendio
Alimentación redundante	NOC (centro Operativo)	EPO (Emergency Power Off – Sistema de corte de energía)	Sprinklers (Rociadores)
Patch panels	Sala de UPS y baterías	Baterías	Extinción por agente limpio (NFPA 2001)
Patch cords	Sala de generador	Monitoreo	Detección por aspiración (ASD)
Documentación	Control de acceso	Generadores	Detección de líquidos
	CCTV	Transfer switch	

2.6 Políticas de Seguridad de la Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de los datos [25].

Las Políticas de Seguridad de la Información son medidas preventivas, que tienen como objetivo gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de las organizaciones.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Una política de seguridad de la información debe expresar el compromiso formal de la administración para la implementación de un sistema de gestión de la seguridad de la información (SGSI), y debe incluir objetivos de seguridad de la información o facilitar su desarrollo.

2.6.1 Normas de seguridad física y ambiental

La protección física y del entorno de ciertas áreas, puede utilizarse como salvaguarda para prevenir accesos no autorizados, pero también es posible de aplicarse a equipos como ser servidores, dispositivos de ruteo y conmutación de datos. También, cumplen una función reactiva, ante ciertos hechos que constituyen riesgos para la seguridad de la información.

La serie de normas ISO 27000 [26], contempla entre sus estándares, objetivos y controles aplicables a la seguridad física y ambiental. Así mismo el marco de trabajo de COBIT [27], permite comprender el gobierno y la gestión de las tecnologías de información (TI) de una organización, e incluye medidas de seguridad física entre sus métricas.

2.6.1.1 Normativa internacional

○ Norma ISO/IEC 27002: 2013 [28]

Es la última edición de la norma internacional, y contiene 14 dominios, 35 objetivos de control y 114 controles. Dentro de los mismos se encuentra el dominio 11 referido a Seguridad Física y Ambiental aplicable a las STS. El mismo está compuesto por dos objetivos de control:

- El objetivo de control 11.1 Áreas Seguras: Los controles descritos en dicho objetivo, apuntan a impedir accesos no autorizados, daños e interferencias a las instalaciones e información de la organización. Y en la cual se recomienda que las instalaciones críticas o sensibles estén ubicadas en áreas seguras, protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de accesos apropiados.
- El objetivo de control 11.2 Seguridad de los Equipos: Los controles descritos en dicho objetivo, apuntan a impedir pérdidas, daños, robos o exposiciones al riesgo de los activos, así como impedir la interrupción de las actividades de la empresa u organismo. Es por ello que recomienda que el equipamiento se encuentre físicamente protegido de las amenazas físicas y del ambiente.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

○ COBIT 5: 2012 [29]

Entre sus procesos de referencia se incluye el de "Gestionar Servicios de Seguridad", con la finalidad de proteger la información de la organización, manteniendo un nivel aceptable de riesgo de seguridad de la información de acuerdo con la política de seguridad. Para ello plasma como meta del proceso implantar medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida, con sus correspondientes métricas relacionadas:

- Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno.
- Clasificación media para las evaluaciones de seguridad física.
- Número de incidentes relacionados con seguridad física.

2.6.1.2 Normativa nacional

- Resolución Nº 048/2005 de la Sindicatura General de la Nación [30]

En su Art. 5 Cumplimiento de Regulaciones Externas, especifica que las unidades responsables de tecnología de información en el sector público, deben garantizar el cumplimiento de las regulaciones relativas a privacidad de la información, propiedad intelectual del software y seguridad de la información.

En su Art. 9 Seguridad, plasma la necesidad de garantizar el cumplimiento de las normas establecidas en cuanto al deber de disponer de una política de seguridad de la información.

Es importante resaltar que es responsabilidad de las áreas de TIC, aplicar Políticas de Seguridad de la Información, que contemplen los controles que permitan normar la seguridad física y ambiental de las salas o cuartos que forman parte de la infraestructura tecnológica de los organismos.

- Norma IRAM ISO/IEC 27002: 2021 [31]

Esta norma es una adopción idéntica de la ISO/IEC 27002: 2013 [28], descripta anteriormente. La edición vigente reemplaza a la IRAM-ISO/IEC 27002: 2008.

- Resolución Nº 829-2019 de Secretaría de Gobierno y Modernización [32]

La vigente normativa aprueba la Estrategia Nacional de Ciberseguridad, la cual establece en su objetivo 5) la protección y recuperación de los sistemas de información del Sector Público, con la finalidad de garantizar que los sistemas de información que utiliza el Sector Público posean un adecuado nivel de seguridad y recuperación.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Al considerar la disponibilidad de los sistemas de información, y que la mayoría de los mismos deben estar accesibles en línea, el servicio de conectividad se vuelve un activo crítico, susceptible a los riesgos que pueden afectar el mismo. En este sentido las STS actuarían como salvaguardas para minimizar el riesgo.

- Disposición Administrativa Nº 641-2021 de la Jefatura de Gabinete de Ministros [33]

La reciente normativa publicada en el boletín oficial de nación, en la Ciudad de Buenos Aires el 25/06/2021, aprueba los requisitos mínimos de seguridad de la información para los organismos del Sector Público Nacional (SPN). El cumplimiento de los mismos será verificado por la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros.

La norma contempla la seguridad física y ambiental en su directriz número 7, y establece que *"los activos de información del organismo deben ser protegidos mediante medidas que impidan accesos no autorizados, daños e interferencia, adoptando suficientes recaudos físicos y ambientales para minimizar los riesgos asociados"* [33].

2.6.1.3 Normativa provincial

- Decreto Nº 1677/2017 del Poder Ejecutivo del Chaco [34]

En su Artículo 1º: Faculta a la Dirección General de Tecnologías de Información a definir, luego del trabajo conjunto con la empresa Ecom Chaco S.A. y el organismo competente de la ejecución de obras, los criterios y especificaciones del diseño de la red de telecomunicaciones en el ámbito de la Administración Pública Provincial. En su Artículo 2º: Establece que la Dirección General de Tecnologías de Información, actuará como órgano de control de la aplicación y cumplimiento de los criterios y especificaciones del diseño de la red de telecomunicaciones, coordinando la ejecución de los lineamientos en materia de seguridad de la información en el ámbito de la Administración Pública Provincial.

Desde el punto de vista normativo plasma las competencias y facultades a la DGTIC, para proponer la implementación de STS como medidas de seguridad de la información.

- Resolución Nº 2515/2017 de la Secretaría General de Gobernación [35]

La normativa instrumentada por la (ex-Secretaría General de Gobierno y Coordinación en la gestión anterior 2015-2019), actual Secretaría General de Gobernación del Poder Ejecutivo

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

del Chaco; aprueba en su Artículo 1º: las etapas del proyecto de "Rediseño, adecuación y saneamiento de la red de datos del edificio de Casa de Gobierno".

La normativa vigente contempla la implementación de STS dentro del proyecto. En particular se destacan tres etapas:

- 3º Etapa: Formulación de estándar tecnológico correspondiente a las STS.
- 4º Etapa: Aprobación de Espacio físico para STS.
- 5º Etapa: Adecuación edilicia del espacio físico para STS.

- Decreto N° 2743/2018 del Poder Ejecutivo del Chaco [36]

Aprueba "Modelo de Políticas de Seguridad de la Información de la Provincia del Chaco". El mismo está basado en Norma ISO/IEC 27002:2013 [28]. La finalidad de dicho instrumento, es facilitar la redacción de políticas a los organismos, brindando una postura provincial sobre los diversos temas que abarca el modelo.

La cláusula 11 Seguridad Física y Ambiental, está compuesta de dos categorías: Áreas Seguras y Seguridad de los Equipos. Ambas con controles aplicables a las STS.

- Ley N° 3203-A de "Simplificación y Modernización Administrativa" [37]

Establece los lineamientos y reglas generales para una administración moderna. Entre los mismos se encuentran el Art. 15: Seguridad de la Información, que comprende al conjunto de políticas, normas, controles, procedimientos, además de la implementación de hardware y software necesarios para preservar la confidencialidad, integridad y disponibilidad de los datos y/o información como activo público de la Administración; y en su Art. 16: Infraestructura tecnológica, promueve implantar una infraestructura tecnológica robusta, escalable, sustentable en el tiempo y eficiente.

2.7 Antecedentes del tema

La revisión de antecedentes estuvo centrada en la investigación de documentos y proyectos relacionados a los sistemas de cableado de telecomunicaciones que aplican directrices, normas, criterios y lineamientos en la implementación de los mismos.

Entre los trabajos relacionados con la temática, se encontraron:

- Mejía Viteri y Murillo Tipán [38], presentan un trabajo de tesis de grado, sobre la implementación de un Data Center Nivel II, para mejorar la infraestructura de la red

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

de una empresa, teniendo la premisa de optimizar los servicios que la misma puede ofrecer en un futuro a sus clientes. Para ello toma en consideración varios aspectos especificados en la norma TIA-942 como son: cableado estructurado, espacios de telecomunicaciones, rutas del cableado, redundancia y un ambiente adecuado para su construcción. Parte de la situación actual de la infraestructura de la red de empresa, y detalla la topología física y lógica, equipos de conectividad, servidores, sistema de cableado estructurado, eléctrico, y plantea un diseño que permita la implementación de nuevos servicios, en base a la infraestructura necesaria para: hosting, videoconferencia y cloud computing.

- Alvarado Tolentino [39], presenta un trabajo de tesis de grado, sobre el diseño de una infraestructura de telecomunicaciones de un municipio, el cual propone la implementación de un centro de datos basado en el estándar ANSI/TIA 942, con el fin de garantizar la seguridad de la información de los servidores del organismo.
- Bastidas Zambrano, Ruíz Parrales y León Acurio [40], presentan una interesante investigación en el libro "Los sistemas de redes en la gestión operativa", donde ponen de manifiesto la falta de aplicación de estándares de calidad requeridos para los sistemas de cableado estructurado. El trabajo investigativo parte de una situación problemática que se basa en la necesidad de complementar las redes internas de los organismos e interconectar los mismos a un sistema general de comunicación de datos de las instituciones públicas. Para ello lleva adelante un cuestionario orientado a: los funcionarios públicos, el personal del departamento de sistemas, y al director del departamento de sistemas.
- Castro Tigua [41], presenta un trabajo de tesis de grado sobre el "Estudio de normas técnicas para la distribución del espacio físico de las instalaciones del laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes". La autora describe los elementos que conforman los estándares ANSI/TIA 568 y 569, luego desarrolla un manual empleando la norma ANSI/TIA 942, y lo aplica a las instalaciones del laboratorio de la facultad.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Las situaciones problemáticas planteadas en los trabajos descriptos plantean la necesidad de aplicación de los estándares de la industria de telecomunicaciones ANSI/TIA. En éste sentido es importante observar que los trabajos de investigación, son en su mayoría tesis de grado publicadas, ya que no se han encontrado trabajos de posgrado sobre implementación de estándares, relacionados a sistemas de cableado de telecomunicaciones y centros de datos.

El principal aporte del presente Trabajo Final de Maestría, es brindar un estudio de posgrado de aplicación práctica basado en los estándares ANSI/TIA 568, 569 y 942, tomando de éstos características de los cuartos de equipos, cuartos de telecomunicaciones, y datacenters, para luego plasmar especificaciones en un modelo de Sala Tecnológica Segura, dentro de un Sistema de Cableado de Estructurado. Es decir que la aplicación de los estándares se aplica al modelo de STS, y luego éste se incluye como parte de un sistema de cableado de telecomunicaciones.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Capítulo 3

Descripción de la problemática

Descripción de la problemática

Partiendo que el diseño de una red de comunicaciones es un marco para la especificación de los componentes físicos de una red y de su organización funcional, configuración, sus procedimientos y principios operacionales, se puede describir la problemática en los organismos públicos del Poder Ejecutivo de la Provincia del Chaco, en base a los siguientes puntos:

1. Problemas en la aplicación de estándares de la industria en materia telecomunicaciones.
2. Falta de propuestas que permitan plasmar políticas, que contemplen inversiones en materia de infraestructura tecnológica robusta, conectividad y seguridad de la información.

Punto 1

En los proyectos de remodelación edilicia de oficinas, o construcción de nuevas áreas en los organismos, se presenta el inconveniente de aplicar correctamente los estándares ANSI/TIA 568, ANSI/TIA-569, ANSI/TIA-942, debido al desconocimiento de los subsistemas que componen un sistema de cableado estructurado, de parte de las áreas técnicas que intervienen en la elaboración de los proyectos ejecutivos.

Siguiendo con la descripción del primer punto, otro inconveniente surge debido al costo de incorporar todos los componentes en la infraestructura, que de acuerdo a ANSI/TIA 568 y ANSI/TIA-569, son:

1. Acometida de entrada
2. Sala o Cuarto de Equipos
3. Cableado vertical o backbone
4. Sala o Cuarto de Telecomunicaciones
5. Cableado horizontal
6. Áreas de trabajo

Esto es particularmente importante ya que la mayoría de los edificios públicos del Poder Ejecutivo de la provincia del Chaco, no contemplan salas o cuartos de equipos para alojar sólo servidores, centrales telefónicas y centrales de video, además de salas o cuartos de

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

telecomunicaciones para ubicar los dispositivos de ruteo y conmutación de la red de datos. Puesto que en la práctica se da, el encontrar en una misma sala o cuarto, los recursos informáticos que deberían estar en la sala de equipos o en la sala de telecomunicaciones.

Punto 2

La modernización de la arquitectura de las redes de los organismos públicos del Poder Ejecutivo de la Provincia del Chaco, no es homogénea. Esto se debe principalmente a la falta de propuestas concretas que plasmen especificaciones, criterios y lineamientos basados en estándares para los sistemas de cableado de telecomunicaciones, en los proyectos de construcción o remodelación que afectan la infraestructura de conectividad.

Es importante resaltar en éste punto, que el Poder Ejecutivo de la provincia del Chaco atraviesa un proceso de simplificación y modernización administrativa [37], pero para dar soporte a los nuevos procesos intra e interinstitucionales, y procedimientos de base digital, se deben desarrollar políticas que contemplen la infraestructura tecnológica y la seguridad de la información.

3.1 Área de conocimiento

El área disciplinar de la presente propuesta de trabajo se enmarca dentro de la asignatura de "Seguridad y Auditoría Informática", de la Maestría en Tecnologías de Información.

Haciendo referencia al modelo de Heckhausen [42], analizando su dominio material, el trabajo se enfoca en las "Tecnologías de Información y Comunicación".

Desde éste enfoque, la tarea de la seguridad informática es la de minimizar los riesgos, que provienen de muchas partes, como ser la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los usuarios, hasta los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad. Así la seguridad debe contemplar tres factores: los usuarios, la información, y la infraestructura.

3.2 Objetivos del Trabajo

3.2.1 General

- Proponer un procedimiento para la implementación de STS (Salas Tecnológicas Seguras) en organismos públicos, a fin de minimizar los riesgos asociados a la seguridad física y ambiental de los sistemas de comunicación de datos, siguiendo un procedimiento basado en estándares.

3.2.2 Específicos

- Analizar la normativa provincial, nacional y estándares internacionales que son de aplicación a las STS.
- Especificar los criterios y lineamientos para la adecuación del espacio físico de las STS, atendiendo a la seguridad física y ambiental, que serán utilizadas en la construcción de las mismas.
- Estimar los costos asociados para la implementación de las STS en organismos públicos, y en particular al edificio de Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco.
- Establecer un procedimiento acorde a las normativas gubernamentales y estándares, para la implementación de STS.
- Evaluar el procedimiento propuesto en un piso del edificio de Casa de Gobierno de la Provincia del Chaco.

3.3 Diagnóstico de la situación actual

En la reciente Ley N° 3203-A [37] aprobada en la provincia del Chaco, se han establecido los principios rectores para la simplificación, racionalización y modernización administrativa, de la Administración Pública Provincial. Sus principios se visualizan en la Figura 5.



Figura 5: Principios Rectores Ley 3203-A [Elaboración propia]

Para aplicar la misma se conformó el Consejo Provincial de Transformación Digital (CTD) [43], con el objetivo de trabajar en una Agenda Digital [44], para promover la modernización del Estado.

Los temas que abarcan los principios rectores, se han agrupado alrededor de 7 ejes principales, entre los cuales se incluyen la Infraestructura Tecnológica y Ciberseguridad como se visualiza en la Figura 6.



Figura 6: Ejes Principales del CTD [Elaboración propia]

Una situación que merece atención es que los temas tratados en el CTD, comparten como raíz un mismo problema: falta de una infraestructura tecnológica robusta, conectividad y seguridad de la información, para dar soporte a los nuevos procesos intra e interinstitucionales, y procedimientos de base digital.

En el marco del CTD, se han conformado comisiones de trabajo para avanzar en los temas inherentes al consejo, las mismas son:

- Modernización Administrativa
- Empleo Público
- Economía del Conocimiento Nuevas Tecnologías
- Infraestructura Tecnológica y Ciberseguridad
- Interoperabilidad e Interconectividad
- Gobierno Abierto
- Gestión por Resultados

Particularmente en la Comisión de Infraestructura Tecnológica y Ciberseguridad, se ha planteado la necesidad de trabajar en la modernización de la arquitectura física y lógica de las redes internas de las jurisdicciones, a fin de ordenar el caos.

3.4 Alcances y limitaciones

Este trabajo fija como alcance la observación de estándares para sistemas de cableado de telecomunicaciones, y la elaboración de especificaciones, criterios y lineamientos a ser aplicados mediante procedimiento a los organismos públicos del Poder Ejecutivo de la Administración Pública Provincial del Chaco. El procedimiento incluye las especificaciones para las Salas Tecnológicas Seguras (STS), también los criterios y lineamientos para un Sistema de Cableado Estructurado (SCE).

Las limitaciones se presentan en términos del presupuesto necesario para la implementación de STS en los organismos públicos, aplicando el procedimiento propuesto para avanzar en la seguridad física y ambiental de las STS dentro de un SCE.

3.5 Metodología

Para el trabajo final de maestría se tomó el enfoque de una investigación cualitativa [45], ya que se busca interpretar como la necesidad de gobernanza en las telecomunicaciones de los organismos públicos de la Administración Pública Provincial del Chaco, se relaciona con la aplicación de políticas que promuevan inversiones en el desarrollo homogéneo de la infraestructura tecnológica, conectividad y seguridad de la información, pero también con la organización de los recursos (humanos y materiales) en los organismos.

En relación al fenómeno, tomando en cuenta la descripción de la problemática y objetivos planteados, surge la siguiente pregunta de investigación:

1. ¿En cuánto afecta a los organismos públicos de la Administración Pública Provincial del Chaco, la falta de una infraestructura tecnológica robusta, conectividad y seguridad de la información, que soporte los nuevos procesos y procedimientos intra e interinstitucionales de base digital?

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Al entender como el aporte normativo de procesos y procedimientos, contribuyen en establecer herramientas para la gobernanza de las telecomunicaciones, promoviendo el desarrollo de una infraestructura digital homogénea en los organismos públicos, podemos obtener conocimiento del abordaje particular a llevar adelante en cada uno de ellos, y sumar a la organización interna necesaria de los mismos, de manera que los nuevos procesos y procedimientos de base digital, se apoyen en una eficiente infraestructura tecnológica, conectividad y seguridad de la información.

La viabilidad de la propuesta de investigación, cuenta con el apoyo de los actores involucrados en el estudio, también con la viabilidad técnica, presupuestaria y política, ya que la misma se enmarca en las en las metas de gobierno.

Los conceptos claves relacionados al fenómeno en estudio se visualizan en la Figura 7.

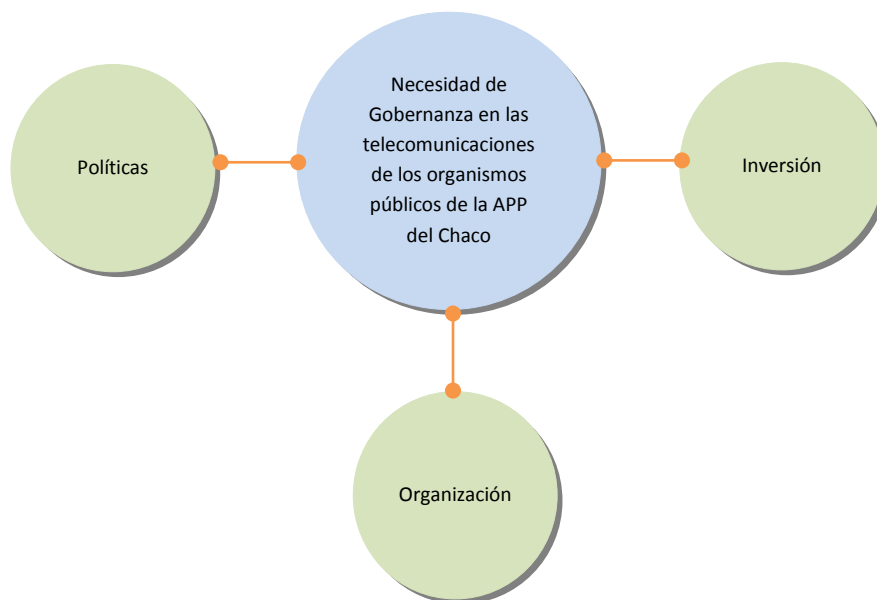


Figura 7: Enfoque cualitativo del fenómeno en estudio [Elaboración propia]

Para situarnos en tiempo y lugar en un contexto de estudio, seleccionamos los organismos públicos que residen en el edificio de Casa de Gobierno de la Provincia del Chaco. Partiendo de una observación inicial del estado general de las redes de datos en los diferentes pisos del edificio, se induce que los organismos mejor organizados, tanto en sus recursos humanos

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

como materiales, tienen mayores posibilidades de aplicar políticas que plasmen propuestas de proyectos, que contemplen inversiones en materia de tecnologías de información.

Para recolectar datos de los individuos involucrados en el estudio, se realizaron entrevistas a referentes informáticos de los organismos, y se instrumentó un formulario de relevamiento (Anexo I) con su correspondiente instructivo (Anexo II).

El reporte de los resultados para el caso de estudio, se basa en un diseño fenomenológico de la investigación [46], y se presenta como informes por piso. En el Anexo III, podemos observar el detalle del informe de la infraestructura tecnológica de un piso de Casa de Gobierno, el cual describe el fenómeno en base a similitudes y diferencias con otros pisos del edificio.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Capítulo 4

Propuesta de solución técnica

Propuesta de solución técnica

Para avanzar en la transformación digital del estado desde la perspectiva de la gobernanza de la infraestructura tecnológica, y como solución a la problemática planteada, se propone trabajar en un procedimiento unificado para implementación de Salas Tecnológicas Seguras en organismos públicos, en el marco de un Sistema de Cableado Estructurado entre los actores con competencia en la provincia, los cuales son:

1. Dirección de Proyectos, dependiente de la Subsecretaría de Planificación y Proyectos de Obras del Ministerio de Planificación, Economía e Infraestructura, del Poder Ejecutivo de la Provincia del Chaco.
2. Dirección General de Tecnologías de Información y Comunicación, dependiente de la Subsecretaría de Modernización del Estado de la Secretaría General de Gobernación, del Poder Ejecutivo de la Provincia del Chaco.
3. Empresa Ecom Chaco S. A.

El procedimiento contará con los siguientes elementos para poder llevarse adelante:

- Especificaciones para las STS, basadas en los estándares ANSI/TIA 568, ANSI/TIA 569 y ANSI/TIA 942. Éstas contemplan la adecuación del espacio físico de las STS, atendiendo a la seguridad física y ambiental, que serán utilizadas en la construcción de las mismas.
- Criterios y lineamientos para el tendido del cableado horizontal de un SCE, basadas en los estándares ANSI/TIA 568 y ANSI/TIA 569.
- Costos asociados a la implementación de las STS.
- Políticas de Seguridad de la Información aplicables a las STS.

4.1 Salas Tecnológicas Seguras

Las STS serán espacios físicos cerrados, con instalaciones eléctricas y contra incendio, mecanismos de control de acceso y condiciones ambientales que puedan albergar, otorgar seguridad y garantizar el funcionamiento de la tecnología informática y recursos de conectividad.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estas condiciones permitirán, en el orden funcional, organizar la conectividad evitando la multiplicidad de equipos de red en diversas oficinas.

4.1.2 Especificaciones para Salas Tecnológicas Seguras

Las especificaciones para las STS, incorporan características de los estándares ANSI/TIA 568, 569 y 942, para que puedan funcionar como salas de equipos y/o salas de telecomunicaciones.

4.1.2.1 Criterios Estructurales

En el diseño se deben tener en cuenta los racks de equipos, incluyendo la gestión del cable junto a los sistemas eléctricos y de refrigeración. Se debe contemplar que los racks estarán llenos y trabajarán de forma eficiente con respecto a los sistemas mencionados.

Dimensiones recomendadas

Respecto a las dimensiones de las salas seguras, se garantizará lo siguiente:

- Deberán permitir el alojamiento del equipamiento tecnológico estimado, de manera estructurada y organizada en su interior. El equipamiento tecnológico estimado deberá considerar el crecimiento de la institución a la que sirve.
- Se debe contemplar espacio adecuado para realizar mantenimiento y reparación, espacio para trabajar y circular cómodamente.
- Debe poseer un espacio suficiente para instalar en su interior: el equipamiento destinado a la misma, el tablero de energía y los sistemas de aire acondicionado, ups, respetando lo requerido en el punto anterior.
- Se recomienda que el despeje (espacio libre) sea al menos de 0,80 m en la parte posterior de los racks y bastidores, y 1 m en la parte delantera de los mismos.
- Se debe prever espacio para una futura ampliación de las instalaciones.

Ubicación y Accesibilidad

En el diseño con respecto a la ubicación física de la STS se debe considerar:

- La facilidad para ingresar elementos de grandes dimensiones, como por ejemplo racks de pie y equipos de alimentación ininterrumpida, entre otros.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- La facilidad de acceso del personal técnico autorizado para solventar cualquier inconveniente emergente.

- Se recomienda que la sala de equipos esté ubicada:
 - Cerca de las canalizaciones de backbone.
 - Donde sea más sencillo y económico distribuir el cableado horizontal hacia los puestos de trabajo (generalmente en el centro de planta).
 - Lejos de fuentes de interferencias electromagnéticas. Ejemplos de dichas fuentes de ruido incluyen el suministro de energía eléctrica, transformadores, motores y generadores, equipo de rayos x, transmisores de radio o de radar, y dispositivos de sellado por inducción.
 - Evitando lugares que restrinjan su futura expansión como ascensores, columnas, tableros principales o entre muros estructurales.
 - Se debe evitar la necesidad de ingresar a otros lugares restringidos para acceder a la sala.

Construcción y Materiales

Considerar lo siguiente en relación a la construcción y los materiales utilizados:

- Si se tratase de una reforma se debe liberar el lugar de todo tipo de instalación preexistente, ajena al funcionamiento de la sala.
- El recinto debe ofrecer resistencia al fuego (RF60).
- El diseño y los materiales deben proporcionar protección anti vandálica de acuerdo al nivel de seguridad requerido.
- Los pisos, las paredes y los techos deberán sellarse, ser pintados o contruidos de un material que logre minimizar el polvo.
- Las terminaciones deberán ser de color claro para mejorar la iluminación de la habitación.
- Puerta: debe proporcionar acceso sólo a personas autorizadas.
 - Debe abrir hacia afuera o deslizarse de lado a lado, de dimensiones mínimas de 0,90 m de ancho y 2,0 m de alto.
 - Se recomienda la instalación de una puerta cortafuego homologada por el INTI [47].

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- Cerradura:
 - Deberá ser reforzada de tipo doble tambor o de tipo vaivén a rodillo.
 - Cuando se estime necesario deberá ser biométrica y estar asociada a un sistema de control de acceso automático que registre fecha y hora de accesos.
 - Deberá garantizar una fácil apertura desde el exterior e interior, sin depender exclusivamente de mecanismos o sistemas electrónicos.
 - Se recomienda la instalación de una barra anti pánico en el interior.
- Piso: Se recomienda que los pisos tengan propiedades antiestáticas.
 - La capacidad de carga del piso en la sala será suficiente para asumir la carga concentrada y distribuida de los equipos instalados con cableado asociado a los medios de comunicación.
- Ventanas: no deben tener ventanas exteriores por motivos de seguridad y para facilitar la correcta refrigeración de la sala.
- Techo: No deberá tener instalado cielorraso, la altura deberá ser de 2,6 m, o mayor a la misma.

Iluminación

- La STS deberá contar con luminarias adecuadas que permitan la operación cómoda sobre el equipamiento alojado.

Canalización

- Se utilizará un esquema, de acuerdo a normas de cableado estructurado (ANSI/TIA 568 y ANSI/TIA 569).
- La STS deberá contar con canales que permitan la correcta gestión del cableado de datos y eléctrico, manteniendo separada la organización de los cables según su función, con una distancia mínima de 30 mm entre los cables de datos y eléctricos.
- La organización del cableado se realizará mediante bandejas que deberán poseer un ancho nominal adecuado para alojar los cables.
- Si se tratase de una instalación nueva, se recomienda dimensionar las bandejas que canalicen el cableado horizontal de datos para que ocupen solamente hasta el 30% de su capacidad, dejando libre lo restante para futuras ampliaciones del cableado.

Protección contra incendios

Se deberá respetar lo siguiente:

- Tener instalado un detector de humo autónomo.
- Tener instalado un detector de temperatura en el interior.
- Tener instalado una baliza luminosa en el exterior.
- Tener instalado una sirena auditiva en el exterior.
- Tener un matafuego de 5 kg Haloclean.
- Sellar la acometida de las instalaciones.

De acuerdo a la criticidad de los servicios relacionados a la sala, cuando se estime necesario, se recomienda implementar un sistema de extinción de fuego automático, que no afecte los dispositivos electrónicos.

Protección contra daños por agua

- Se recomienda que el piso de la STS posea un nivel elevado con respecto a la planta general.
- Los equipos en la STS deberán estar instalados de forma elevada del nivel del piso. Se deberá construir un sistema de drenaje apropiado.
- Se deberá instalar los equipos de manera que queden protegidos de humedad, inundaciones y goteras.
- Eliminar caños de agua o desagües en el área de la sala segura, o factores que puedan generar humedad.
- Se deberá instalar un sensor de humedad.

Energía

- Las instalaciones eléctricas deberán realizarse de acuerdo a las normativas de la AEA [48], y considerando estándares aplicables a la situación particular.
- Se deberá prever la instalación de tomacorrientes cercanos a donde serán ubicados los racks, dispositivos a utilizar en la sala, y otros de uso libre para herramientas eléctricas, por ejemplo, equipo de limpieza.
- La tensión de alimentación de los dispositivos informáticos, deberá provenir desde una línea eléctrica exclusiva.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- Dicha línea debe ser de uso exclusivo para los dispositivos implementados en la STS, de manera que no deberá ser accesible a elementos externos a la misma o dispositivos dentro de la STS que no cumplan funciones relacionadas a los servicios críticos de la sala.
- Se recomienda la alimentación mediante grupo electrógeno ante cortes de energía, permitiendo que las cargas críticas sólo sean expuestas a apagones durante mantenimientos preventivos o correctivos.
- Tablero de energía: Deberán tener un tablero de energía que permita el control para la administración del suministro de energía eléctrica de manera local. La construcción e instalación de dicho tablero deberá realizarse de acuerdo a las normativas de la AEA [48], aplicable a la situación y deberá verificarse según los criterios establecidos en la misma. Los circuitos de alimentación eléctrica de las luminarias, refrigeración, sistemas auxiliares y activos de red deberán ser debidamente organizados, y rotulados de manera independiente en el tablero.
- Puesta a tierra: Cada STS deberá poseer una red de puesta a tierra que se ajuste a las normas. Cada rack deberá estar conectado a la red de puesta a tierra de acuerdo a las normas correspondientes.

Se deberá prever la separación y disposición adecuada entre las puestas a tierra de los dispositivos electrónicos y la de los dispositivos eléctricos.

Condiciones ambientales

- Las STS deberán contar con un sistema de refrigeración, alimentado por una línea eléctrica independiente a la de los dispositivos de conectividad, que permita controlar los siguientes problemas ocasionados por condiciones ambientales inadecuadas:
 - Temperaturas altas y bajas
 - Control de humedad relativa
- El sistema de refrigeración se encontrará disponible durante las 24 horas de los 365 días del año.
- Se deberá dimensionar la cantidad de frigorías/watts del acondicionador, realizando el cálculo correspondiente, teniendo en cuenta la energía disipada en forma de calor por el equipamiento instalado, además de los valores de temperatura interior y

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

exterior. En ningún caso se dispondrá de un valor inferior a las 70Fgs/m³ ni un equipo acondicionador de capacidad inferior a las 4500Fgs/h.

- El sistema de refrigeración deberá ser ubicado, de manera que asegure la integridad de las instalaciones eléctricas y electrónicas de la sala.
- Se deberá prever el desagote de agua producida por condensación.
- Se recomienda efectuar la instalación de la unidad interior del sistema de refrigeración sobre la puerta de acceso a la sala.
- Cuando se estime necesario se recomienda el uso de equipos redundantes de refrigeración que trabajen de manera automatizada.

4.1.2.2 Criterios de Seguridad

Control de acceso

- Se deberá restringir el acceso a la sala a todo personal ajeno a la operación o mantenimiento de la misma.
- Se deberá asegurar el acceso a todo responsable de operación o mantenimiento de la sala, o al personal encargado de atender cualquier tipo de emergencia.
- Se recomienda implementar un sistema que permita el control y el registro de fecha y hora de los accesos físicos a la sala.

Videovigilancia

Se deberá monitorear mediante videovigilancia, de manera que sea posible visualizar la totalidad del interior de la STS respetando lo siguiente:

- Calidad: se debe visualizar con una resolución de 1280x1024 píxeles y 25-30 fps (cuadros por segundo), o con una resolución mayor.
- Grabación: deberá contar con la opción de activar detección de movimiento.
- Administración: la tecnología deberá ser administrada por un responsable o área asignada.
- Archivado: se recomienda almacenar las transmisiones de video en un medio interno a la sala (NVR), accesible por el personal a cargo de la misma.

Sistema de alimentación ininterrumpida

Se deberán prever los errores de operación, o fallas de los componentes de infraestructura que causen interrupciones en los servicios.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

La STS deberá incluir un sistema de alimentación ininterrumpida, soportado por una o varias unidades UPS, considerando los siguientes aspectos:

- Las unidades UPS deberán disponerse de forma estructurada y organizada, para su fácil acceso y administración, integrándose a la distribución de equipamiento de la STS.
- Las unidades UPS serán aptas para el funcionamiento con la tensión y frecuencia de la red eléctrica de las instalaciones (tensión y frecuencia de entrada), y brindarán la tensión adecuada según las especificaciones del equipamiento que alimenta (tensión y frecuencia de salida).
- Las especificaciones de las unidades UPS deberán ajustarse a los requerimientos detectados, a partir de las especificaciones de los equipos alojados en la STS y la necesidad de disponibilidad de los mismos.
- Las unidades UPS deberán poseer indicaciones de encendido y de pérdida de energía primaria.
- Las unidades UPS deberán poseer sistemas de seguridad ante sobrecarga.
- Se recomienda el tipo senoidal de doble conversión y en línea.

Sistema de monitoreo

- Se recomienda instalar sistemas o tecnologías que se encarguen de recolectar datos entre los diferentes componentes implementados en la STS, como son el sistema de detección de incendio, la alimentación eléctrica, los servicios de red, las condiciones ambientales, el control de acceso y la videovigilancia, permitiendo monitorear el estado de los diferentes componentes de las salas para la correcta gestión de la infraestructura.

Documentación

Se deberá asegurar la existencia de:

- Planos de construcción y preinstalaciones.
- Plano del cableado eléctrico.
- Plano del cableado de la red de datos.
- Inventario e identificación de los racks y el equipamiento.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

4.1.2.3 Diseño físico de la red de datos

El diseño físico de la red de datos interna, de los organismos que conforman la Administración Pública Provincial, deberán respetar la topología en estrella, ya que éste define la interconexión de las estaciones de trabajo y el camino de transmisión de datos sobre el medio de comunicación.

El diseño deberá nacer en el router de cabecera del piso u organismo, a éste se deberá conectar el switch de stacking o agregación, luego los switches de distribución se deberán conectar al switch de agregación, y finalmente las estaciones o puestos de trabajo se deberán conectar a los switches de distribución. El objetivo es, obtener mayor rendimiento y velocidad de la red, y consecuentemente mejorar la productividad de los usuarios.

De acuerdo a las necesidades de conectividad, se deberá realizar el diseño previo, plasmando en planos gráficos el despliegue de la red de datos, como se visualiza en las topologías de los ejemplos de la Figura 8, 9 y 10.

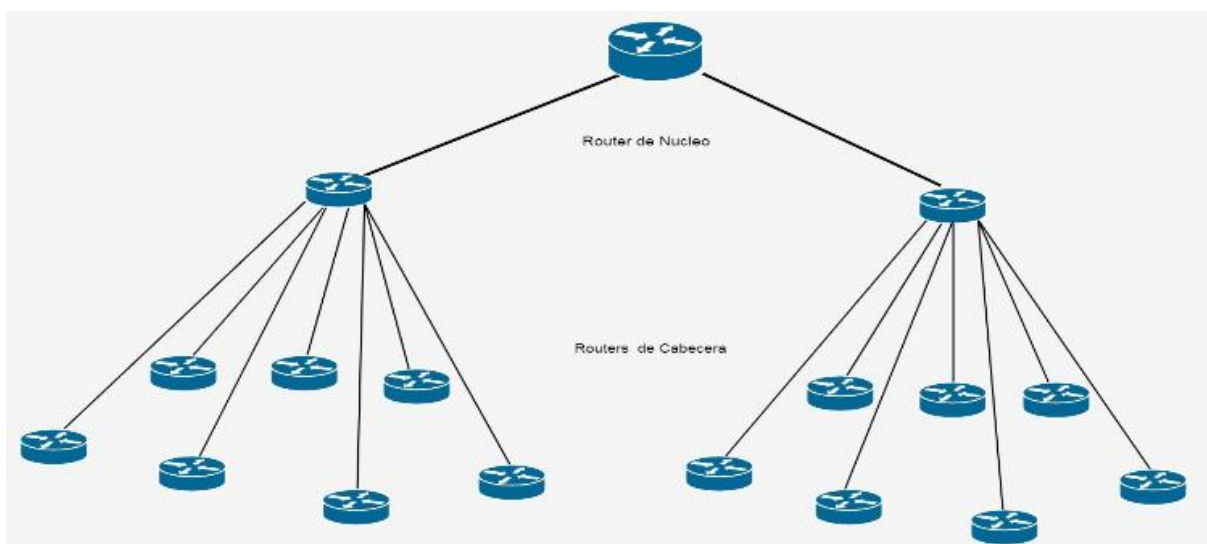


Figura 8: Topología 1 [Elaboración propia]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

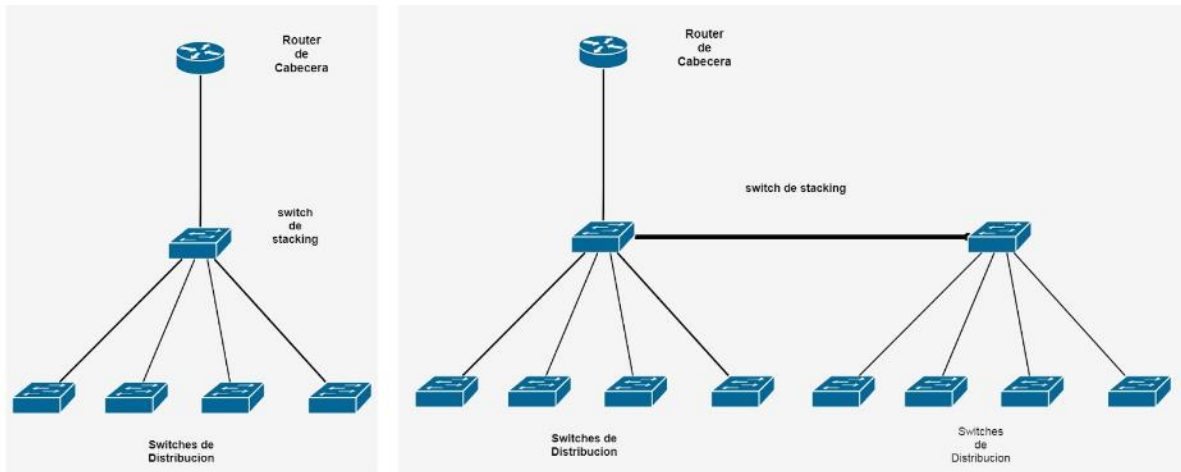


Figura 9: Topología 2 [Elaboración propia]

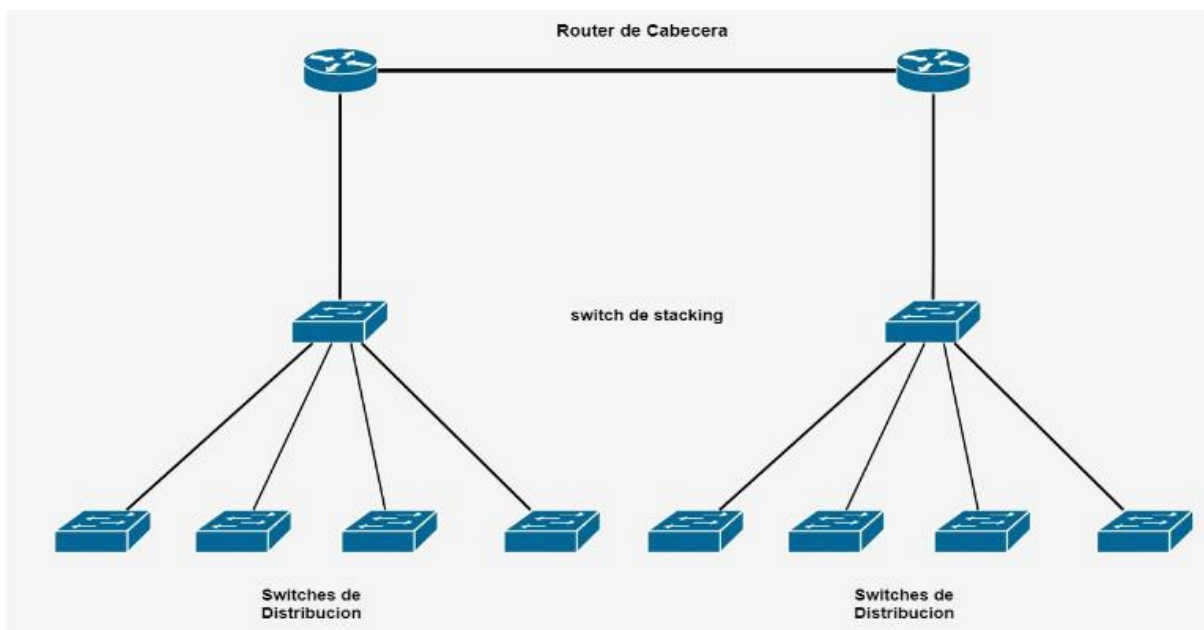


Figura 10: Topología 3 [Elaboración propia]

4.1.2.4 Obra Civil de STS

La adecuación edilicia es un elemento prioritario en la ambientación de las STS, ya que contempla las características constructivas que hacen a la seguridad física y ambiental, protegiendo a éstos espacios de potenciales riesgos como ser acceso no autorizado, vandalismo, hurto, entre otros. A continuación, se plasma un resumen de la obra civil a llevar adelante en la construcción de las STS.

Tabla 2: Obra civil STS [Elaboración propia]

ORDEN	RUBRO	DESCRIPCIÓN DE OBRAS
1	CONSTRUCCION EN SECO	Pared Doble FR60 Placa EST 12,5 mm FR60. Estructura perf. Cal. 0,52 mm. Refuerzos para equipos de AA y tableros. Lana de vidrio 50 mm
2	PISO	Baldosas de goma 50x50 3,2 mm Tipo Deco de Indelval
3	ZÓCALOS	Zócalo de MDF prepint. 70 mm de altura, 3,4" esp. Sin molduras
4	PINTURA	Pintura látex para interiores
		Esmalte sintético sobre puerta metálica.
		Pintura de losa existente
		Pintura Identificación STS Piso y unidad
5	CARPINTERÍAS	Puerta de rebatir (910x2200) RF60 Rejilla vent. Barral antipánico; Burletes;
6	INSTALACIÓN ELÉCTRICA	Tablero Eléctrico de corte General, monofásico
		Artefactos de Ilum. Marea LED, instalado
		Bocas de luz
		Toma exterior
		Toma A20
		Artefacto luz de emergencia, instalado
		Puesta a Tierra
		Bandejas Datos y Energía
		Alimentación desde TGP (Tablero General del Piso) hasta tablero de sala, con protección.
7	SISTEMA DE REFRIGERACIÓN	Provisión y Montaje un (1) Aire Split AA 4500 fg/h frio solo. Clase A. Gas Eco. R410a. Autoencend. Auto-diag. Falta gas refrig. Bloqueo del equipo cuando disminuye carga del líquido ref. Garantía 2 años.
8	CONTROL DE ACCESO y CCTV	Cerrojo digital biométrico y tarjeta. La cerradura podrá ser del tipo Anviz, modelo: VF30, denominación: Fingerprint Access Control.
		Carteles de Salida, Señalética seguridad, instalado
9	INSTALACIONES CONTRA INCENDIOS	Sensor de Temperatura, instalado
		Sensor de humo, instalado
		Central de Incendio, 1 lazo, convencional, instalada
		Matafuego ABC 5 kg, IRAM, baliza. Carga vigente 1 año.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

4.1.2.5 Elementos y Electrónica de Conectividad de STS

Se deberá contemplar que la velocidad de transmisión de datos en cada puesto sea de 1 Gbps, para ello la electrónica de conectividad deberá ser administrable. Los dispositivos de red administrables permitirán implementar medidas de seguridad lógica en la red del piso u organismo al que pertenecen.

Para tener una idea más aproximada de la electrónica y elementos de conectividad a contemplar en una cotización, se plasma una recomendación de los mismos en la siguiente tabla.

Tabla 3: Electrónica y elementos de conectividad [Elaboración propia]

CATEGORÍA	ÍTEM Y DESCRIPCIÓN	OBSERVACIONES
Equipamiento TIC Sala Tecnológica Segura	Módulo SFP+ Mikrotik para conexión de racks centrales con racks secundarios.	Por unidad (2 por conexión)
	Router de Cabecera: Debe contener un puerto de fibra sfp +. Fuente redundante de alimentación.	Por unidad Modelos de ejemplos de acuerdo al tráfico a manejar: Mikrotik Ccr1016-12s-1s+
	Switch de Agregación: interconecta los switches de distribución	Por unidad Modelos de ejemplos de acuerdo al tráfico a manejar y al puerto utilizado: SFP+: Mikrotik 317-1G-16S+RM
	Switch de Distribución: 24 puertos de gigabits. Administrable. Con puerto SFP.	Por unidad Modelo de ejemplo: Mikrotik CRS326-24G-2S+RM
	Equipo NVR: Kit Seguridad NVR de 4 canales + 2 Cámaras Hd Exterior + disco de almacenamiento preparado para grabación continua	Por unidad
	UPS rackeable: administrable 1,5 KVA batería interna	Por unidad
Elementos de cableado estructurado en Sala Tecnológica Segura	Rack de 19": 45 unidades	Por unidad Modelo de ejemplo: Rack Evo Iv 45u 1000mm Gabitel R-e4-45u
	Rack de 19": 12 unidades	Por unidad

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

	Rack de 19" : 6 unidades	Por unidad
	Canal de tensión : 5/6 tomas con llave térmica	Por unidad
	Patch panel Cat. 6 24 puertos	Por unidad
	Patch panel Cat. 6 48 puertos	Por unidad
	Organizador de cables 2u	Por unidad
	Bandeja Metálica : Para Rack 19" 2U	Por unidad
	Cable SFP-SFP+ . Para conexión de backbone.	Por unidad Modelos de ejemplos de acuerdo a la distancia entre dispositivos: Direct attach de 5 mts Direct attach de 3 mts Direct attach 2 mts Direct attach de 1 mts
	Patch Cords cat. 6 de 0.50 cm.	Por unidad
	Patch Cords cat. 6 de 1 m.	Por unidad
	Mano de Obra	En horas

La electrónica y elementos de conectividad de la infraestructura de red propuesta, plasma una administración centralizada de los dispositivos ruteo y conmutación (routers y switches), con la debida protección por UPS (sistema de alimentación ininterrumpida), organizados en un rack principal como se visualiza en la Figura 8.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

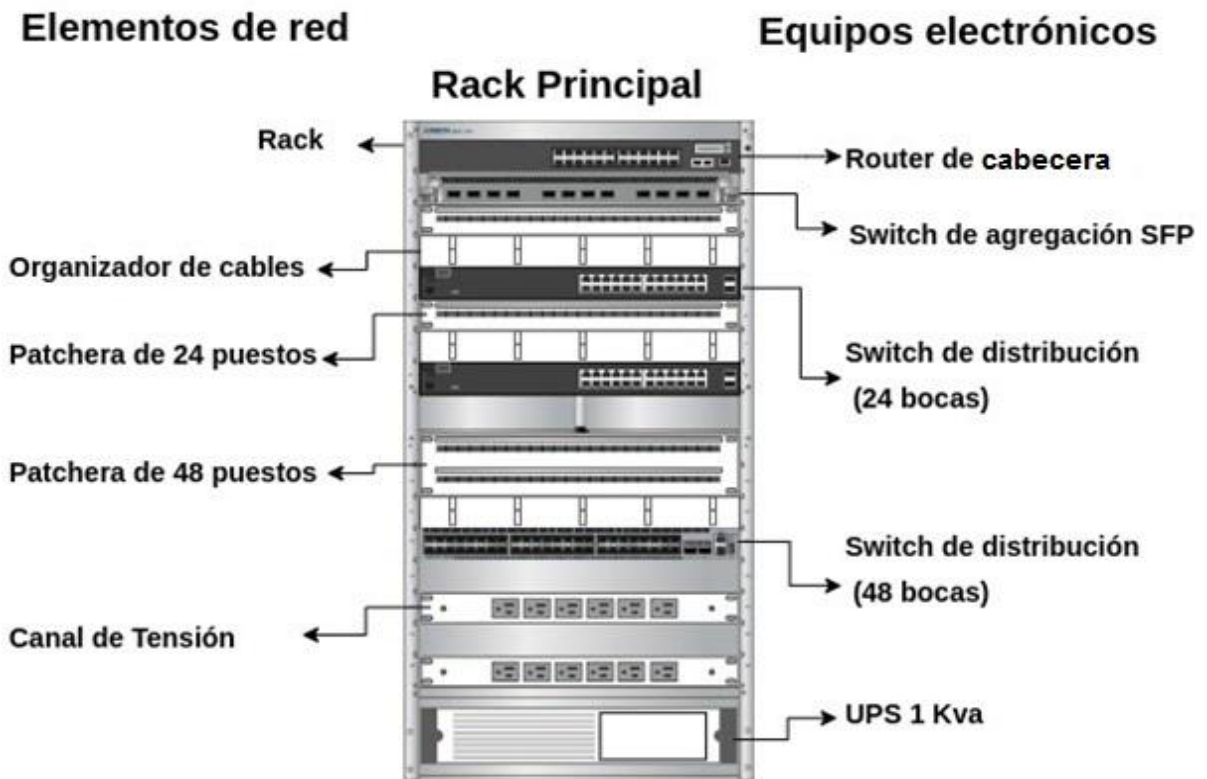


Figura 11: Organización de rack principal [Elaboración propia]

4.1.2.6 Modelos 2D de Sala Tecnológica Segura

La arquitectura de las STS responde a los criterios estructurales y de seguridad planteados en el punto 4.1.2.1 y 4.1.2.2, como se visualiza en las Figuras 12 y 13.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

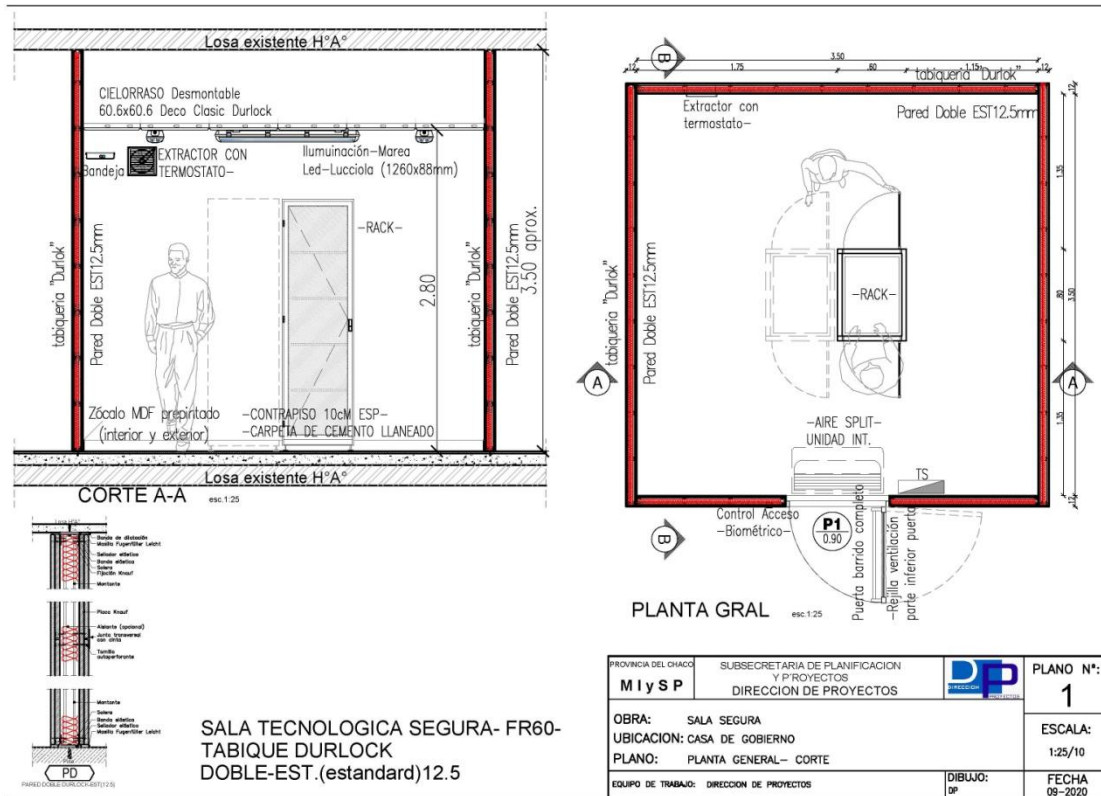


Figura 12: Planta General - Corte [Elaboración propia]

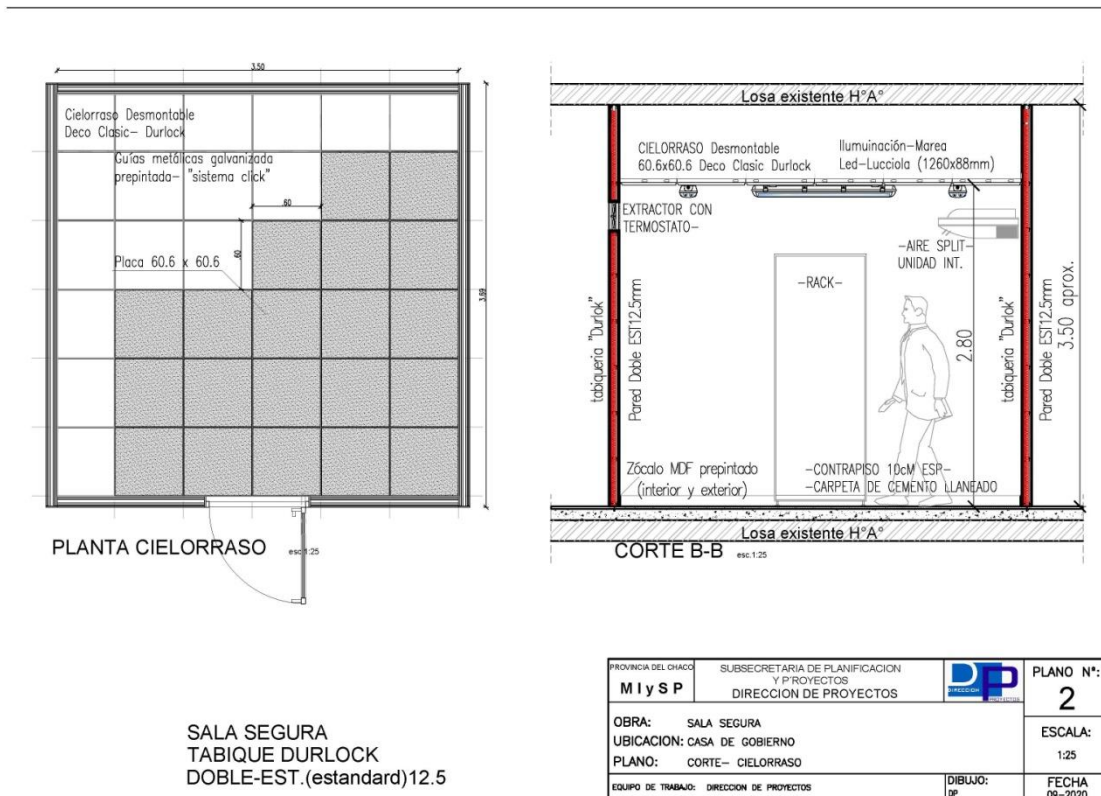


Figura 13: Corte - Cielorraso [Elaboración propia]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

4.1.2.7 Modelos 3D de Sala Tecnológica Segura

Así mismo, la organización de las STS responde a los criterios estructurales y de seguridad planteados en el punto 4.1.2.1 y 4.1.2.2, como se visualizan en las Figuras 14, 15, 16, 17, 18 y 19.

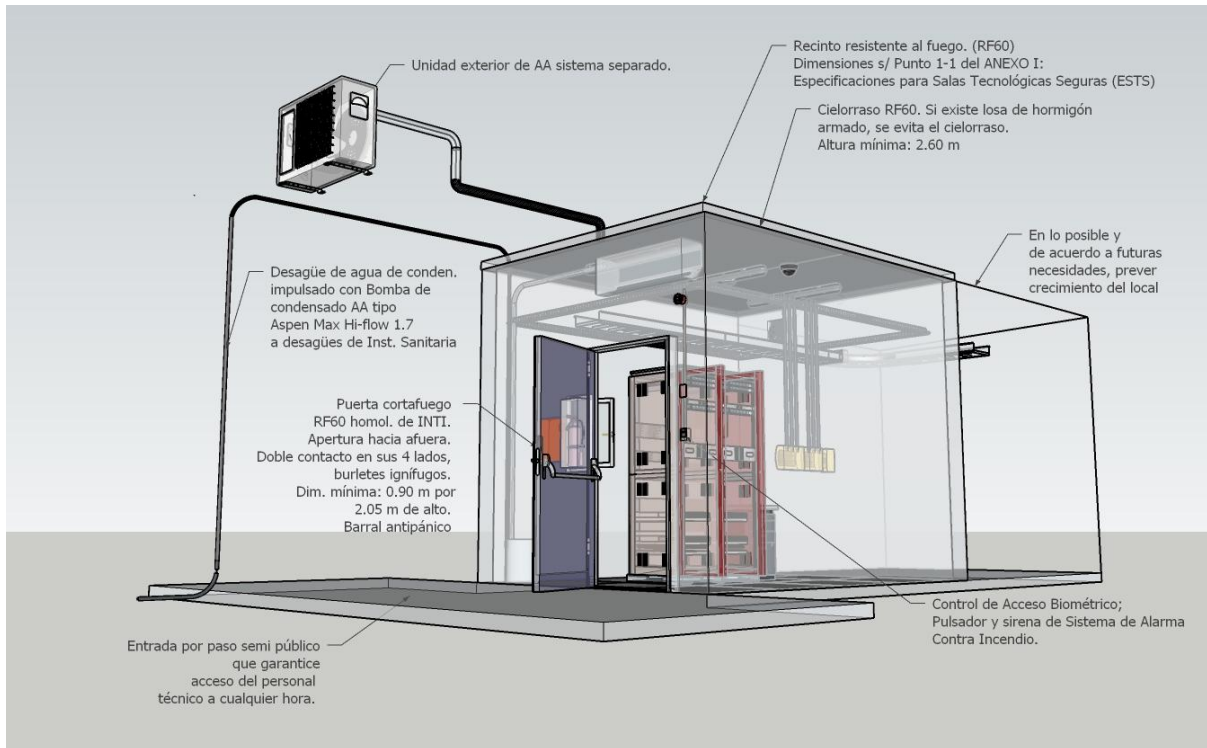


Figura 14: Vista interna de STS [Elaboración propia]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

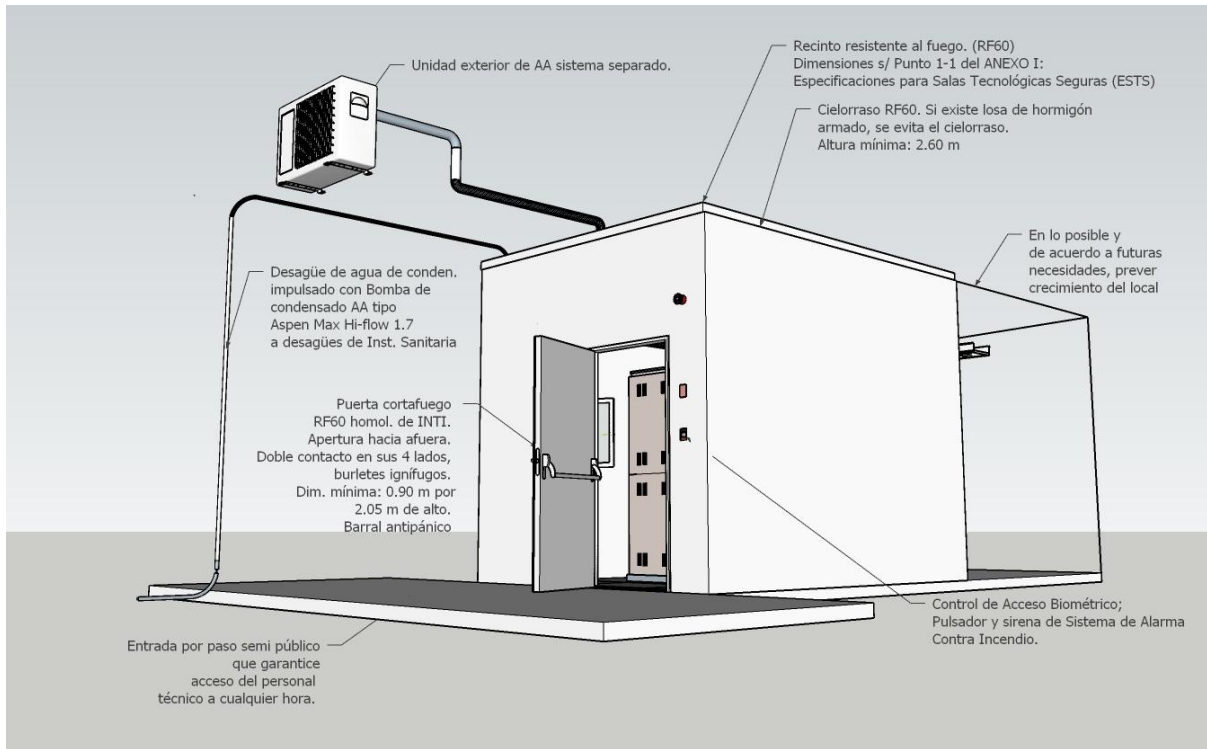


Figura 15: Vista externa de STS [Elaboración propia]

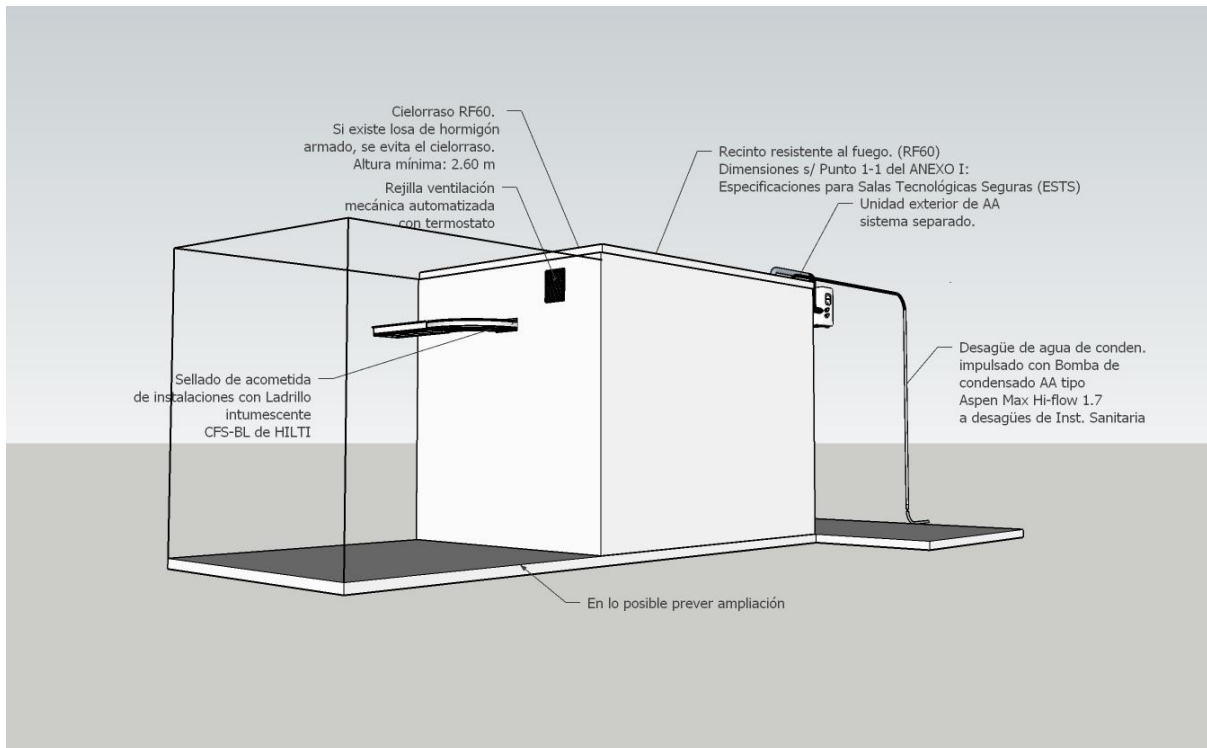


Figura 16: Vista de STS ampliada [Elaboración propia]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

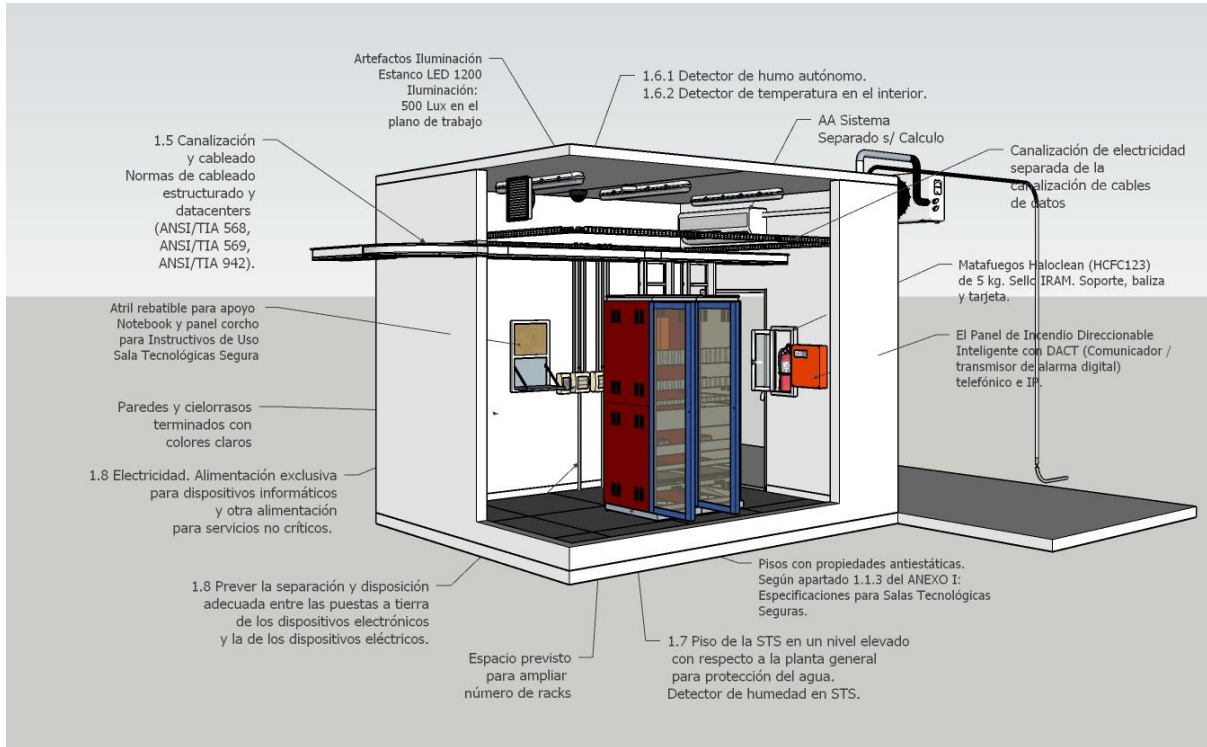


Figura 17: Vista lateral con corte de STS [Elaboración propia]

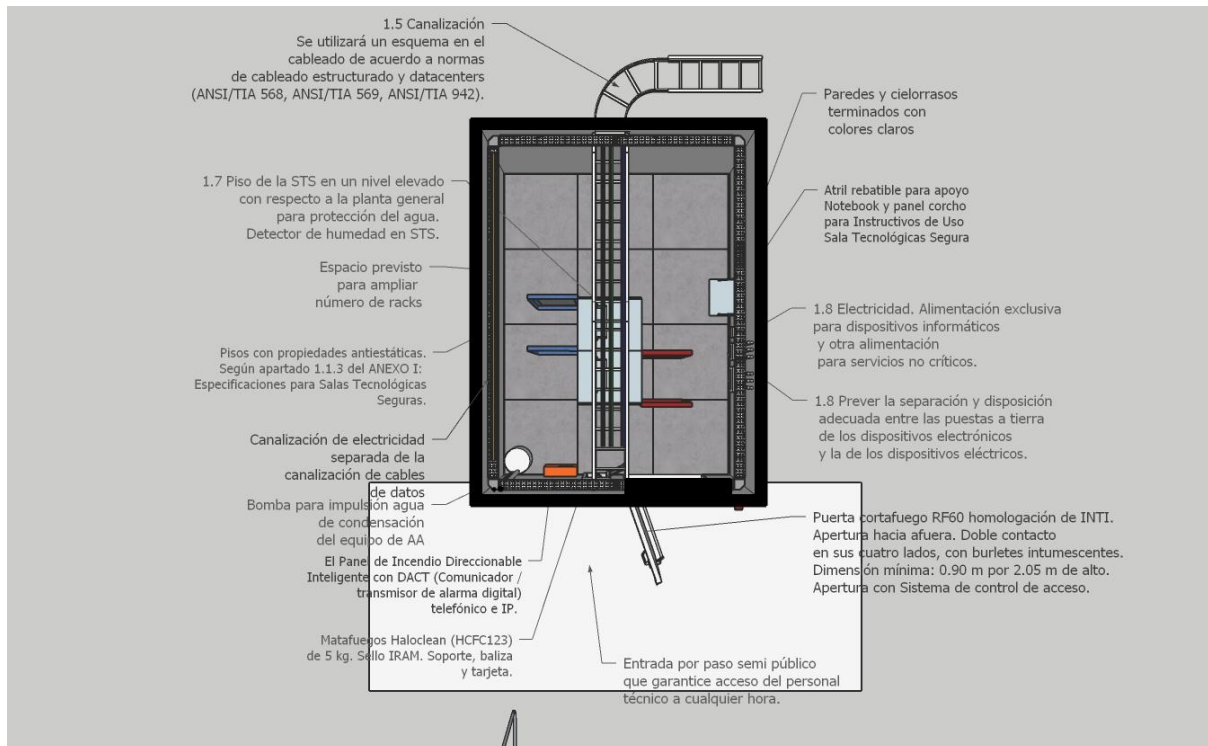


Figura 18: Vista superior de canalización de STS [Elaboración propia]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

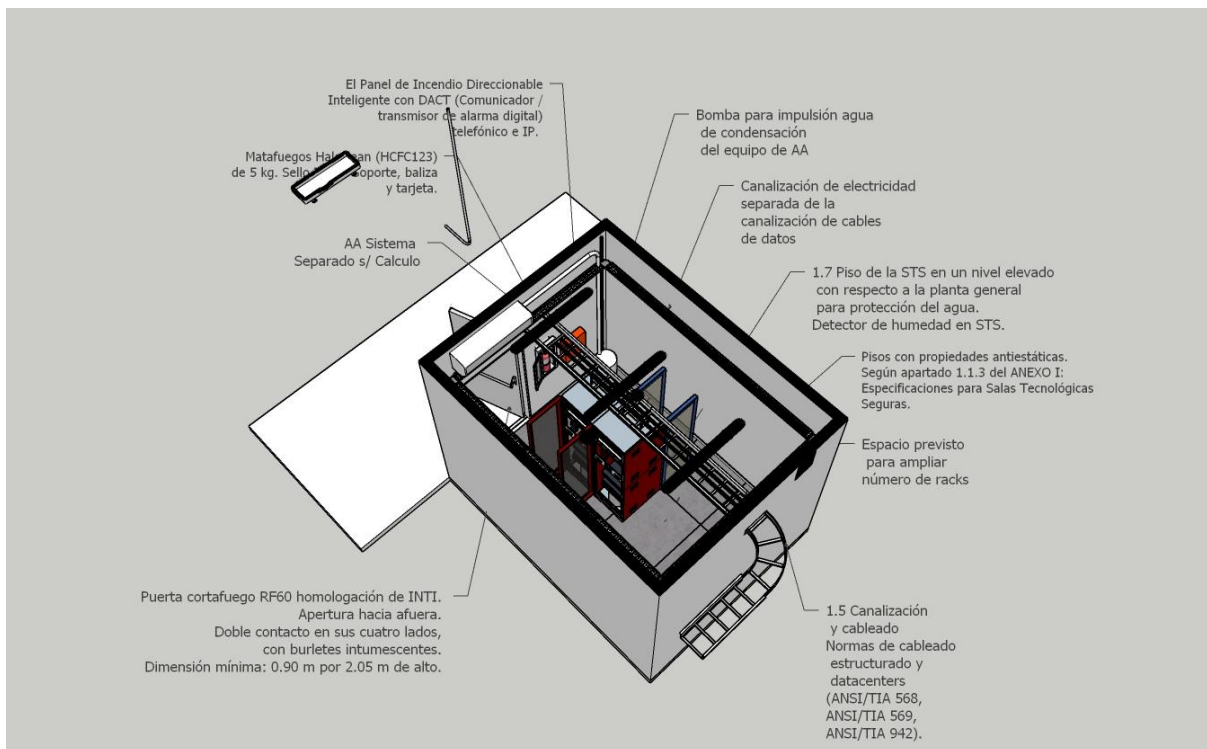


Figura 19: Vista superior inclinada de canalización de STS [Elaboración propia]

4.2 Sistema de Cableado Estructurado

Un SCE constituye la infraestructura ordenada de cables, conectores, canalizaciones y equipos, que permite transportar las señales digitales desde un equipo transmisor hasta un equipo receptor. El mismo debe ser pensado y proyectado para tener una vida productiva entre 15 a 25 años. En este período, las tecnologías de telecomunicaciones seguramente cambiarán varias veces. Por ello, el diseño del cableado deberá prever grandes anchos de banda, y ser adecuado tanto a las tecnologías actuales como a las futuras.

4.2.1 Criterios para un Sistema de Cableado Estructurado Horizontal

Los criterios y lineamientos para un SCE se ajustan a los estándares ANSI/TIA 568, y ANSI/TIA 569, siendo aplicables para un piso, un organismo, edificio o el cableado entre edificios de una misma red.

4.2.1.1 Diseño del cableado

La categoría requerida del cable UTP deberá ser 6 o superior:

- En proyectos que contemplen nuevo cableado estructurado.
- En proyectos que contemplen el reemplazo del cableado estructurado.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- En proyectos que agreguen puestos de trabajo, a los ya existentes en una oficina u organismo.

Los elementos a adquirir (cables, conectores, y paneles) deberán ser de la misma categoría.

En proyectos que contemplen la reutilización del cableado estructurado, se deberá verificar el buen funcionamiento del mismo, admitiéndose sólo aquél que se encuentre en buen estado.

El cableado deberá seguir una topología tipo estrella jerárquica, con centro en la Sala Tecnológica Segura (STS), y cada uno de los extremos ubicados en las áreas de trabajo.

El cableado deberá finalizar en la STS o rack principal del mismo piso del área a la que se está dando servicio.

El cableado horizontal incluye: el cable UTP, área de trabajo, terminaciones mecánicas, conectores y patch cords situados en la Sala Tecnológica Segura.

En el tendido del cableado horizontal se pueden incluir dispositivos MUTO o Puntos de Consolidación.

La distancia máxima para el cableado de distribución horizontal es de 100 metros, donde 90 metros se considera desde la boca de red, a la cual se conecta el área de trabajo, hasta el patch panel de interconexión en el rack ubicado en la Sala Tecnológica Segura.

Los patchs cords utilizados en las áreas de trabajo y en el rack de la Sala Tecnológica Segura no deben ser más largos de 5 metros, es decir en conjunto no deberán ser mayores a 10 metros, como se visualiza en la Figura 20.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

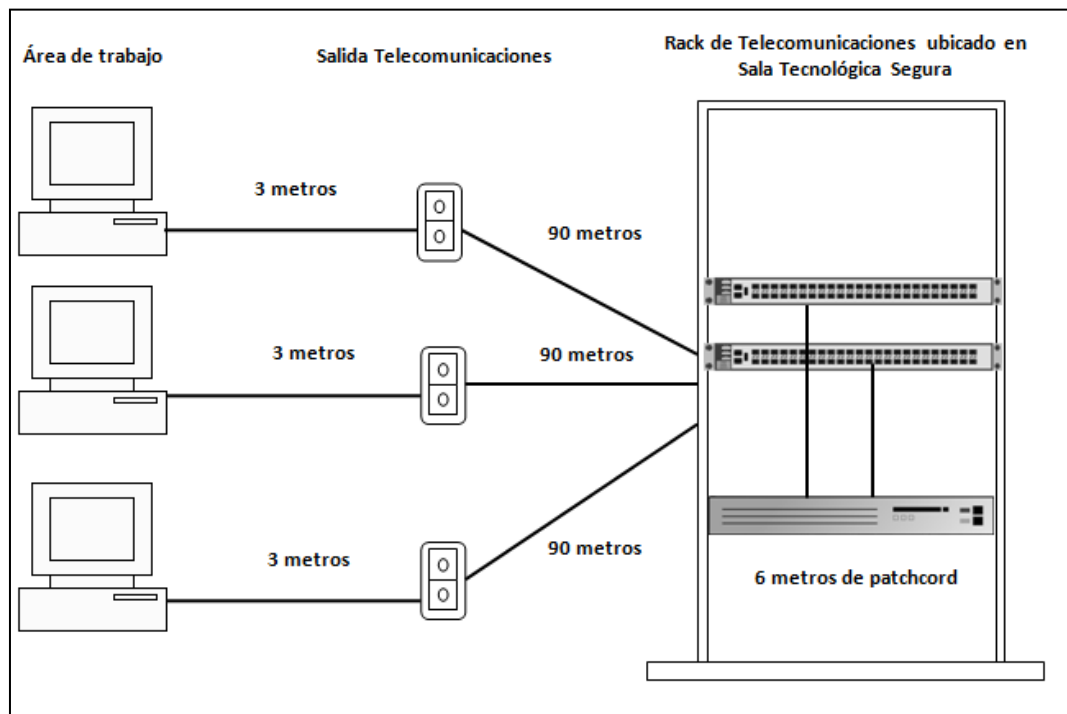


Figura 20: Distancias máximas para el cableado horizontal [49]

4.2.1.2 Cableado horizontal en oficinas abiertas

Las prácticas de diseño de oficinas abiertas utilizan conjuntos de terminales de telecomunicaciones multiusuario (MUTO), puntos de consolidación (CP), o ambos para proporcionar diseños flexibles.

MUTO: Son equipos que permiten a los usuarios trasladarse, agregar equipos y realizar cambios en la distribución de los muebles modulares sin la necesidad de volver a tender el cableado.

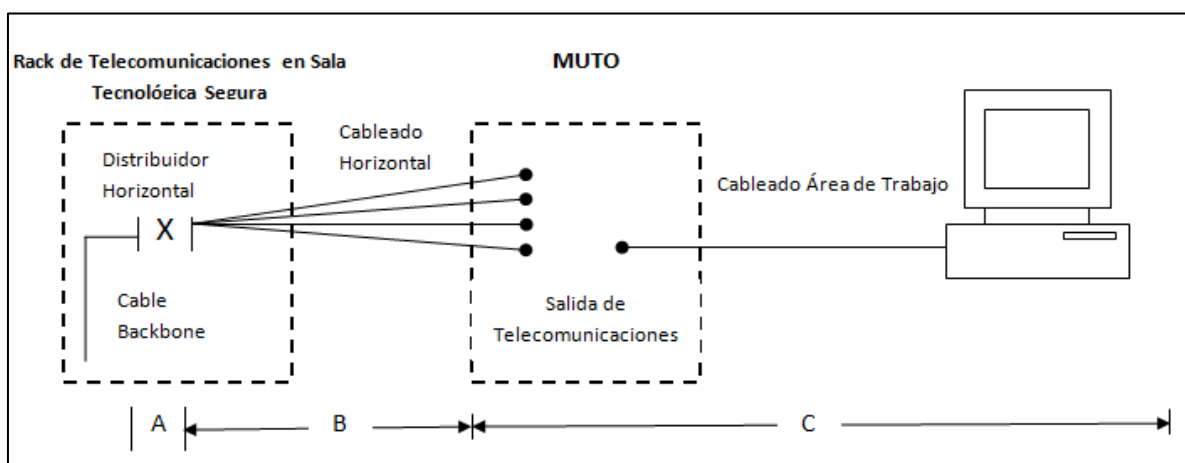


Figura 21: MUTO [50]

Las distancias máximas admisibles utilizando un dispositivo MUTO son:

Tabla 4: Distancias máximas admisibles con un dispositivo MUTO [50]

Tramo A	Tramo B	Tramo C	Distancia total
5	90	5	100
5	85	9	99
5	80	13	98
5	75	17	97
5	70	22	97

Puntos de consolidación o CP: Es una interconexión en el cableado horizontal que permite configuraciones más sencillas en oficinas abiertas con muebles modulares. El punto de consolidación utiliza hardware de conexión instalado. A diferencia del MUTO, requiere una conexión adicional para cada recorrido del cable horizontal.

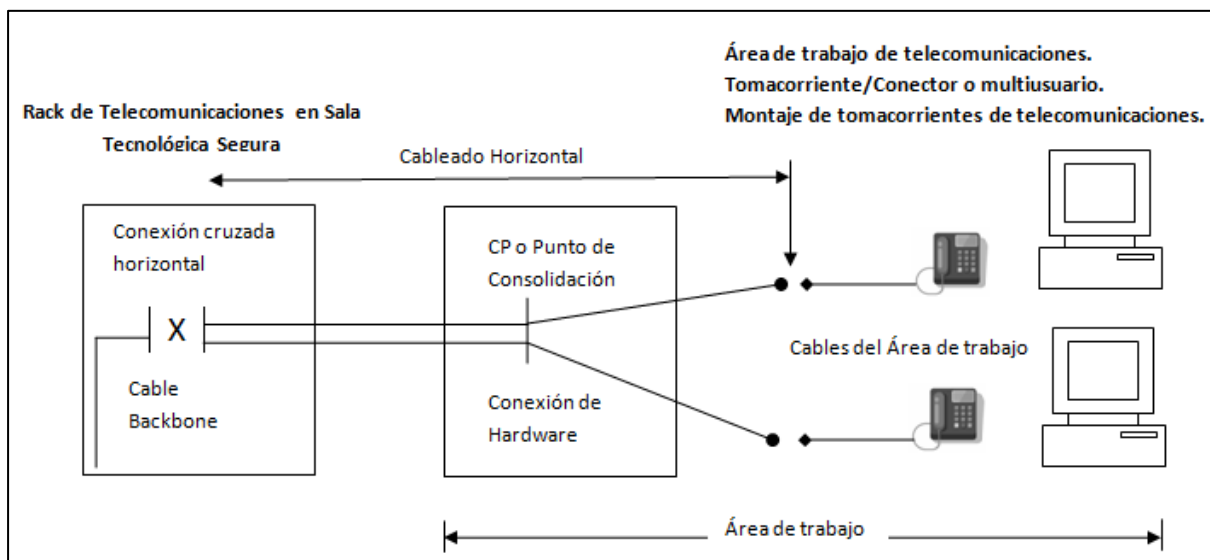


Figura 22: Punto de consolidación [50]

Los CP no pueden estar a menos de 15 metros de la Sala Tecnológica Segura, y no puede haber más de un CP entre cada corrida de cable.

4.2.1.3 Canalizaciones horizontales

Las canalizaciones horizontales son aquellas que unen las STS o racks con las áreas de trabajo. Estas canalizaciones deberán ser diseñadas para soportar los tipos de cables, entre los que se incluyen el cable UTP de 4 pares, el cable STP y la fibra óptica.

El estándar ANSI/TIA 569 admite los siguientes tipos de canalizaciones:

- Ductos bajo piso
- Ductos bajo piso elevado
- Aparentes
- Bandejas
- Sobre cielorraso
- Perimetrales

4.2.1.4 Elementos y materiales para despliegue del cableado horizontal

Para tener una idea más aproximada de los elementos y materiales para el despliegue del cableado horizontal a contemplar en una cotización, se plasma en la siguiente tabla un listado de los mismos.

Tabla 5: Elementos del cableado horizontal [Elaboración propia]

CATEGORÍA	ÍTEM Y DESCRIPCIÓN	OBSERVACIONES
Elementos de cableado estructurado en distribución de la planta	Gabinete de 19": 12 unidades	Por unidad
	Gabinete de 19": 6 unidades	Por unidad
	Bandeja portacable de 100 mm.	Por unidad
	Bandeja portacable de 300 mm.	Por unidad
	Bandeja portacable de 400 mm.	Por unidad
	Soporte tipo trapecio para bandeja portacable de 100 mm.	Por unidad
	Soporte tipo trapecio para bandeja portacable de 300 mm.	Por unidad
	Soporte tipo trapecio para bandeja portacable de 400 mm.	Por unidad
	Varilla Roscada de 8mm con sus respectivas tuercas y arandelas.	Por unidad
	Taco metálico p/hormigón 8mm	Por unidad
	Reducción para bandeja portacable: de 300 a	Por unidad

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

	200 mm.	
	Empalme para bandeja portacable	Por unidad
	Curva plana de 90º para bandeja portacable de 400 mm.	Por unidad
	Derivación universal para bandeja portacable de 2 piezas, ancho variable.	Por unidad
	Curva vertical articulada para bandeja portacable de 400 mm.	Por unidad
	Unicanal 100x50 mm (se usa como referencia Hellermann Tyton)	Por unidad
	Faceplate para 4 tomas rj-45 para unicanal	Por unidad
	Caja de cable de 305 mts. Cat. 6 (referencia: Furukawa)	Por unidad
	Jack RJ-45 Cat. 6 (referencia: marca GLC)	Por unidad
	Patch Cords cat. 6 de 1 m.	Por unidad
	Mano de Obra	En horas

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Capítulo 5

Procedimiento para la implementación de Salas Tecnológicas Seguras

Procedimiento para la implementación de Salas Tecnológicas Seguras (STS)

El procedimiento comprende una sección de consideraciones generales, y otra donde se describen los componentes del procedimiento, con su correspondiente flujograma.

5.1 Consideraciones Generales

Objeto

Establecer un procedimiento unificado para la implementación de Salas Tecnológicas Seguras.

Ámbito de aplicación

El ámbito de aplicación de este procedimiento se circunscribe a los organismos públicos de la Administración Pública Provincial del Poder Ejecutivo de la Provincia del Chaco.

Abreviaturas y definiciones

- **MAJ:** Máxima Autoridad Jurisdiccional.
- **MPEI:** Ministerio de Planificación, Economía e Infraestructura.
- **SPP:** Subsecretaría de Planificación y Proyectos de Obras.
- **DP:** Dirección de Proyectos.
- **DGTIC:** Dirección General de Tecnologías de la Información y Comunicación
- **ECOM:** Empresa Ecom Chaco S.A.
- **JUR:** Refiere a la jurisdicción u organismo donde se implementará la Sala Tecnológica Segura.
- **STS:** Sala Tecnológica Segura.
- **PEF:** Propuesta de Espacio Físico.
- **PEO:** Proyecto Ejecutivo de Obra
- **RI:** Responsable Informático

Análisis de la infraestructura tecnológica

Para realizar un análisis de la infraestructura tecnológica de los organismos públicos, priorizando la seguridad física y ambiental de los espacios para alojar servidores, electrónica y elementos de conectividad, se propone catalogar las redes de los organismos en 3 niveles:

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

1. *Red sin administración:* La misma está compuesta por elementos de enrutamiento y conmutación que pueden o no estar alojados en rack de comunicaciones, y no posee una topología claramente definida. No existe una adecuada organización en cuanto a la administración de los dispositivos de red: routers, switches de agregación y switches de distribución. Lo cual presenta múltiples puntos susceptibles de fallos y de riesgos físicos. No existe la figura de un administrador de red o un equipo técnico que haga sus veces.
2. *Red con administración descentralizada:* La misma posee una topología mixta o híbrida, por lo cual pueden coexistir dos o más topologías de red diferentes. Esta topología contiene una combinación de la topología de bus, topología de malla, topología de anillo y topología de estrella. Por lo cual puede haber subredes administradas por diferentes administradores de red o equipos técnicos.
3. *Red con administración centralizada:* La misma posee una topología estrella o estrella extendida, es administrada por un administrador de red o un equipo técnico que haga sus veces, con la existencia de un rack de comunicaciones principal, del cual pueden desprenderse conexiones hacia:
 - Las áreas de trabajo.
 - Rack de comunicaciones secundarios.

Relevamiento

Para plasmar informes de la infraestructura tecnológica de los organismos, se realizaron entrevistas a los responsables informáticos de los mismos, y se utilizó un formulario de relevamiento (ver ANEXO I, e instructivo ANEXO II), el cual presenta 4 secciones como se visualizan en la siguiente tabla.

Tabla 6: Secciones del formulario de relevamiento [Elaboración propia]

Secciones	Descripción
Sección 1: Datos Generales	Se busca entrevistar al Responsable Informático designado para responder las preguntas acerca de la Infraestructura Tecnológica del organismo.
Sección 2: Servidores	Se busca relevar datos sobre los servidores que tenga el organismo.
Sección 3: Cuartos de Equipos/Comunicaciones	Se busca relevar datos sobre los cuartos de equipos/comunicaciones que alojan servidores y/o equipos de comunicaciones.
Sección 4: Red Interna	Se busca relevar datos sobre el estado de la red interna del organismo.

Estimación de Riesgos

Luego del relevamiento de la infraestructura tecnológica del organismo, se analizaron los datos y se realizó una estimación de riesgos.

Tabla 7: Riesgos de la infraestructura tecnológica [Elaboración propia]

Ítem	Riesgo	Detalle
Servidores	Servidores sin respaldo de datos	Los servidores no cuentan con medio de respaldo de datos. En caso de fallas se perderían los mismos.
	Los servidores no cuentan con una protección energética (UPS)	Los equipos no poseen ups en su mayoría, quedando expuestos a fallas o pudiendo llegar a quemar los mismos.
Cuartos de equipos/comunicaciones	Espacio físico no delimitado	Los servidores y equipos de comunicaciones no están alojados en un espacio seguro, quedando expuestos al acceso no autorizado, a daños naturales por fuego, agua, y a daños intencionales.
	Conexiones eléctricas deficientes	Los cuartos de equipos y/o comunicaciones no poseen una línea eléctrica independiente, quedando expuestos a fallas en la alimentación del suministro.
Sobre la red interna	Cableado de red no documentado	Se carece de planos de redes, de etiquetados y rotulados, lo cual dificulta la ubicación de bocas en mal estado o fuera de funcionamiento.
	Red no administrada	El organismo no cuenta con personal interno o externo que administre la red, lo cual dificulta la aplicación de políticas de seguridad de la información.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

5.2 Componentes del procedimiento

El procedimiento propuesto para la implementación de STS, contempla 3 componentes:

1. Informe de la infraestructura tecnológica.
2. Construcción - obra civil de la STS.
3. Adquisición de electrónica y elementos de conectividad para la STS.

5.2.1 Descripción gráfica del procedimiento

El esquema gráfico de la Figura 23, muestra la secuencia entre los componentes del procedimiento.

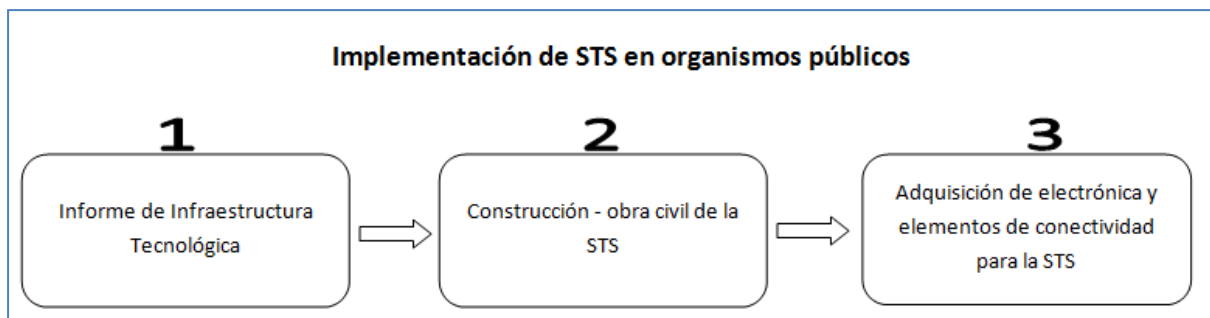


Figura 23: Secuencia de componentes del procedimiento [Elaboración propia]

5.2.2 Diagrama de flujo del procedimiento

A continuación, se visualiza el diagrama de flujo del procedimiento (DFP) de los pasos a seguir, teniendo en cuenta la secuencia de los 3 componentes plasmados en las Figuras 24, 25 y 26.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

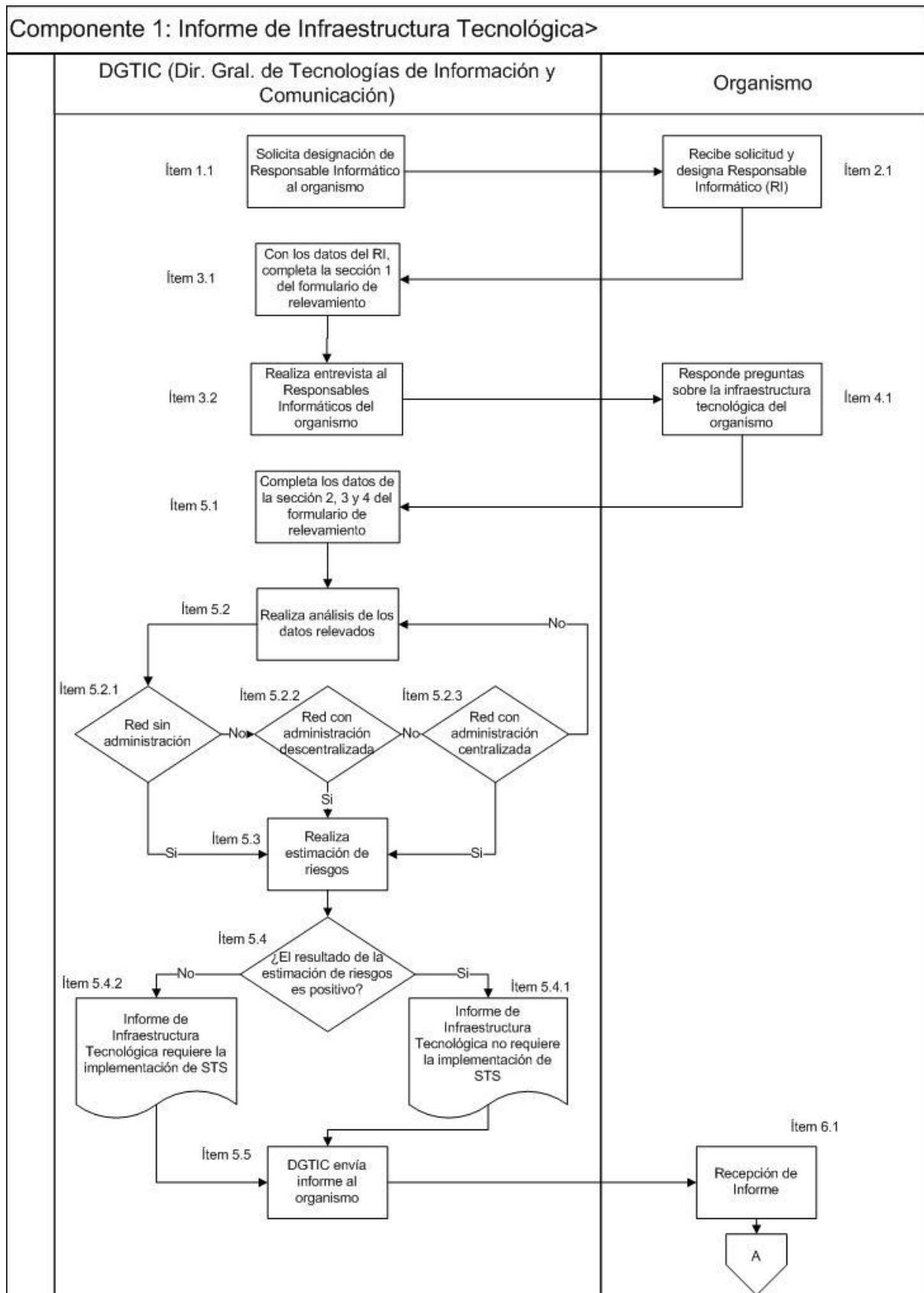


Figura 24: DFP del Informe de Infraestructura Tecnológica [Elaboración propia]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

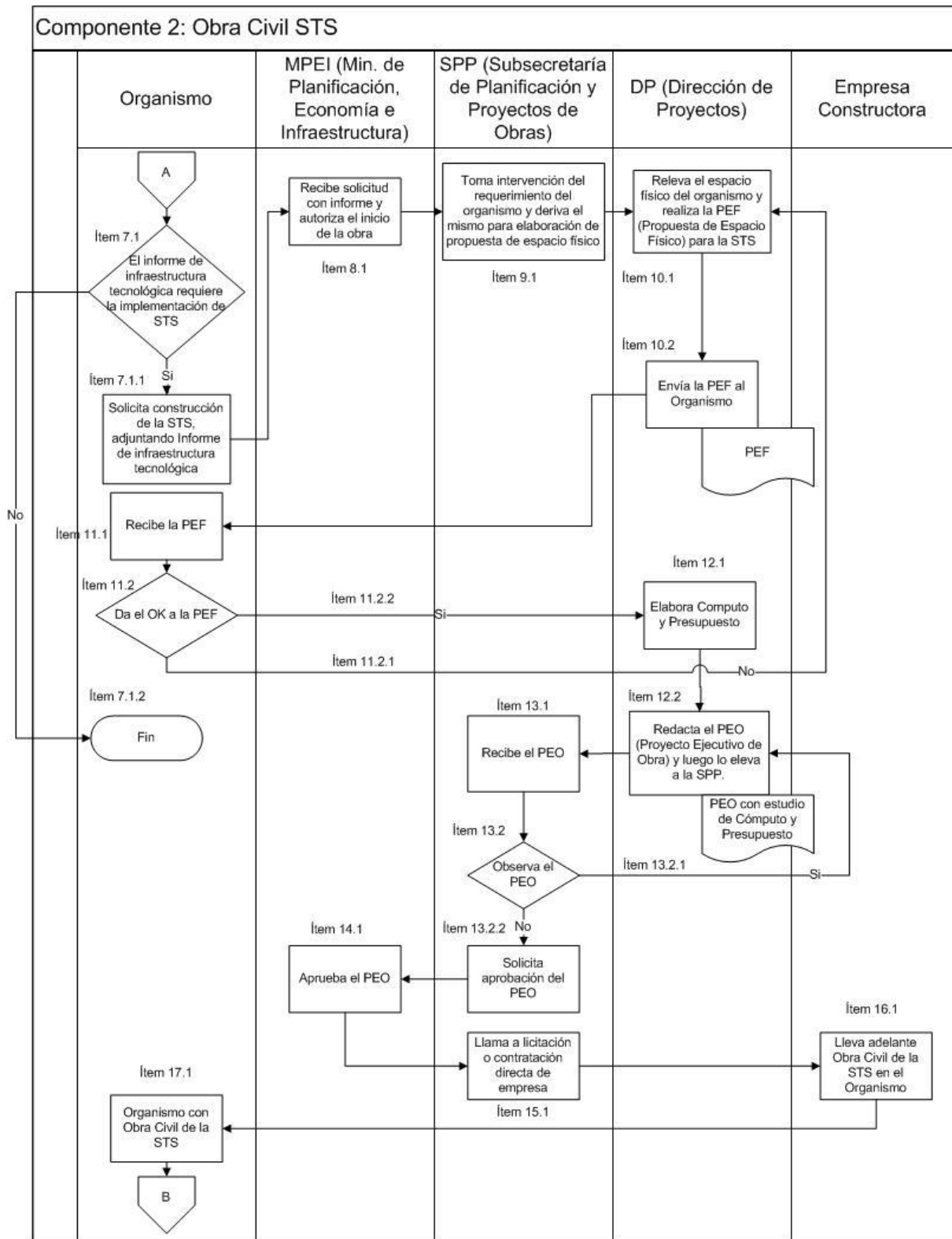


Figura 25: DFP de la Obra Civil de la STS [Elaboración propia]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

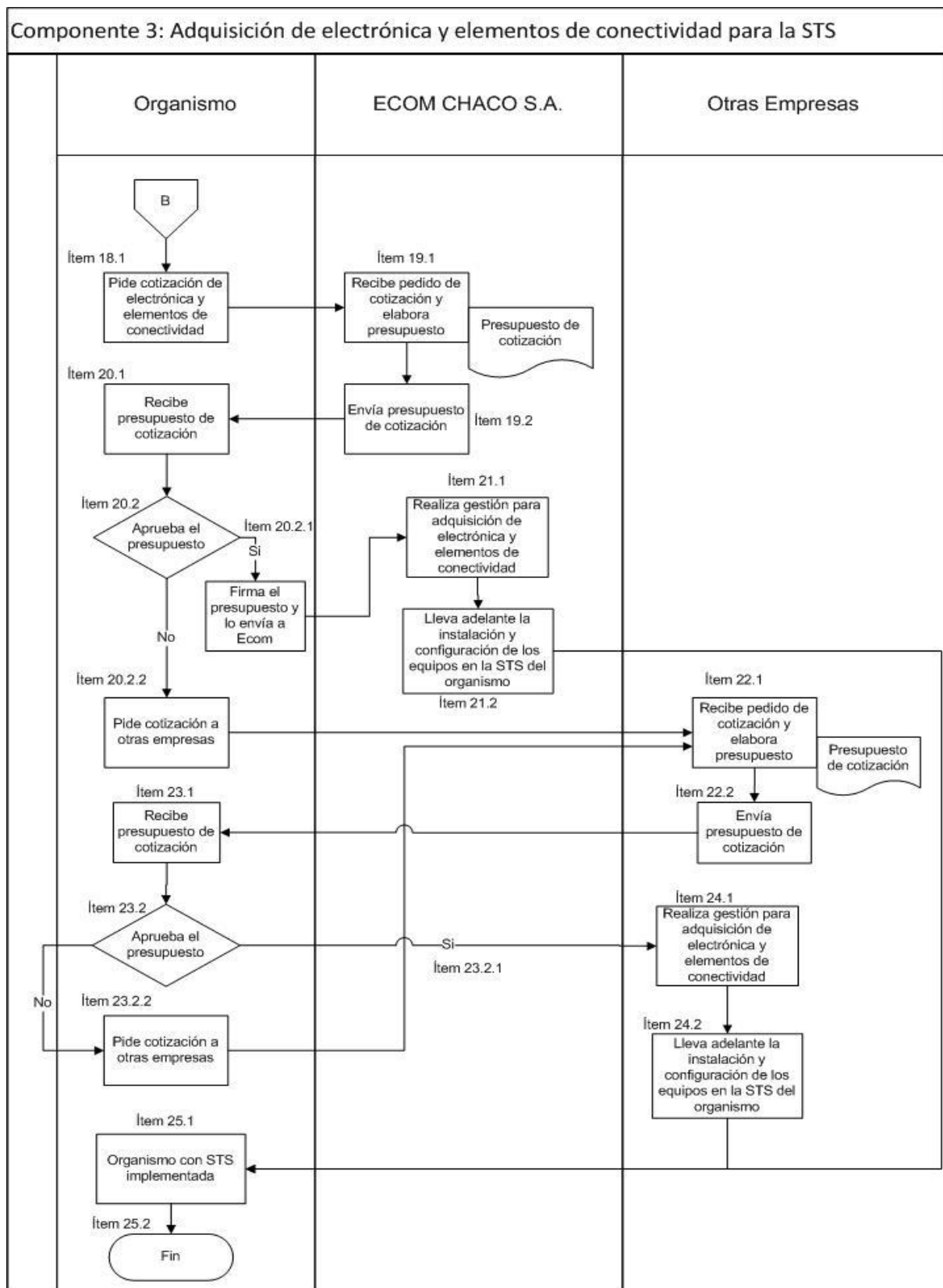


Figura 26: DFP de la adquisición de electrónica y elementos de conectividad para la STS [Elaboración propia]

5.2.3 Descripción detallada del procedimiento

Componente 1: Informe de la infraestructura tecnológica

1. Área DGTIC

1.1 La DGTIC solicita designación de Responsable Informático al organismo.

2. Área JUR

2.1 La JUR recibe solicitud y designa Responsable Informático (RI).

3. Área DGTIC

3.1 La DGTIC recibe la designación del RI, y con los datos del mismo completa la sección 1 del formulario de relevamiento.

3.2 Luego personal de la DGTIC realiza entrevista al RI designado del organismo.

4. Área JUR

4.1 El RI responde preguntas sobre la infraestructura tecnológica del organismo.

5. Área DGTIC

5.1 Con las respuestas del RI, el personal de la DGTIC completa los datos de la sección 2, 3 y 4 del formulario de relevamiento.

5.2 Luego la DGTIC realiza análisis de los datos relevados, y categoriza la infraestructura tecnológica del organismo en:

5.2.1 Red sin administración

5.2.2 Red con administración descentralizada

5.2.3 Red con administración centralizada

5.3 Luego la DGTIC realiza una estimación de riesgos de los datos relevados.

5.4 El resultado de la estimación de riesgos puede ser:

5.4.1 Positivo: El Informe de Infraestructura Tecnológica que plasma la DGTIC, no requiere la implementación de STS en el organismo.

5.4.2 Negativo: El Informe de Infraestructura Tecnológica que plasma la DGTIC, requiere la implementación de STS en el organismo.

5.5 Luego la DGTIC envía Informe de Infraestructura Tecnológica al organismo.

6. Área JUR

6.1 La JUR recibe el informe.

Componente 2: Construcción - obra civil de la STS

7. Área JUR

7.1 Analiza respuesta del Informe de Infraestructura Tecnológica realizado por DGTIC:

7.1.1 Si el informe recepcionado requiere la implementación de STS en el organismo, la JUR solicita la construcción de la STS al MPEI, adjuntando Informe de infraestructura tecnológica de la DGTIC. Continúa en el ítem 8.1.

7.1.2 Si el informe recepcionado no requiere la implementación de STS en el organismo, entonces finaliza el procedimiento.

8. Área MPEI

8.1 Recibe solicitud con informe, autoriza el inicio de la obra, y da intervención a la SPP.

9. Área SPP

9.1 Toma intervención del requerimiento del organismo y deriva el mismo a la DP, para la elaboración de la PEF (Propuesta de Espacio Físico) para la STS.

10. Área DP

10.1 Releva el espacio físico del organismo y realiza la PEF (Propuesta de Espacio Físico) para la STS.

10.2 Luego envía la PEF a la JUR del organismo.

11. Área JUR

11.1 La JUR recibe la PEF, y comunica a la MAJ (Máxima Autoridad Jurisdiccional).

11.2 La MAJ de la JUR analiza la PEF y expresa su definición:

11.2.1 No aprueba la PEF: La JUR comunica sus observaciones de la PEF a la DP, y envía la actuación. Regresa al ítem 10.1.

11.2.2 Aprueba la PEF: La JUR envía la actuación a la DP, para la elaboración de Cómputo y Presupuesto. Continúa en ítem 12.1.

12. Área DP

12.1 Si la PEF de la DP, tuvo la aprobación de la JUR, entonces la DP elabora Cómputo y Presupuesto de la misma.

12.2 Luego la DP redacta el PEO (Proyecto Ejecutivo de Obra) con estudio de Cómputo y Presupuesto, y lo eleva a la SPP.

13. Área SPP

13.1 Recibe el PEO y analiza el mismo:

13.2 Analiza el PEO enviado por la DP:

13.2.1 Si el PEO tiene observaciones, se deriva el PEO junto con sus observaciones nuevamente a la DP, para subsanar las mismas. Regresa al ítem 12.1.

13.2.2 Si el PEO no tiene observaciones, la SPP solicita la aprobación del mismo a la MAJ del MPEI. Continúa en ítem 14.1.

14. Área MPEI

14.1 Si el PEO no tiene observaciones de la SPP, entonces la MAJ del MPEI aprueba el PEO, y deriva el mismo a la SPP.

15. Área SPP

15.1 La SPP con el PEO aprobado, realiza la gestión para el llamado a licitación o contratación directa de empresa para la construcción de la obra civil de la STS.

16. Empresa Constructora

16.1 Lleva adelante Obra Civil de la STS en el Organismo.

17. Área JUR

17.1 El organismo queda con la Obra Civil de la STS finalizada.

Componente 3: Adquisición de electrónica y elementos de conectividad para la STS

18. Área JUR

18.1 La JUR pide cotización de electrónica y elementos de conectividad para la STS a la empresa Ecom Chaco S.A.

19. Empresa Ecom Chaco S.A.

19.1 Recibe pedido de cotización y elabora presupuesto.

19.2 Luego envía presupuesto a la JUR.

20. Área JUR

20.1 Recibe presupuesto de cotización enviado por Ecom.

20.2 Analiza el presupuesto de cotización:

20.2.1 Aprueba el presupuesto: Firma la aprobación del presupuesto y lo envía a la empresa Ecom Chaco S.A. Continúa en el ítem 21.1.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

20.2.2 No aprueba el presupuesto: La JUR pide cotización a otras empresas.

Continúa en el ítem 22.1.

21. Empresa Ecom Chaco S.A.

21.1 Con el presupuesto aprobado por la JUR, realiza gestión para adquisición de electrónica y elementos de conectividad para la STS.

21.2 Luego de la adquisición, lleva adelante la instalación y configuración de los equipos en la STS del organismo. Continúa en el ítem 25.1.

22. Otras Empresas

22.1 Recibe pedido de cotización y elabora presupuesto.

22.2 Luego envía presupuesto a la JUR.

23. Área JUR

23.1 Recibe presupuesto de cotización enviado por empresa

23.2 Analiza el presupuesto de cotización:

23.2.1 Aprueba el presupuesto: Firma la aprobación del presupuesto y lo envía a la empresa. Continúa en el ítem 24.1.

23.2.2 No aprueba el presupuesto: La JUR pide cotización a otras empresas. Retorna al ítem 22.1.

24. Otras Empresas

24.1 Con el presupuesto aprobado por la JUR, realiza gestión para adquisición de electrónica y elementos de conectividad para la STS.

24.2 Luego de la adquisición, lleva adelante la instalación y configuración de los equipos en la STS del organismo. Continúa en el ítem 25.1.

25. Área JUR

25.1 El organismo queda con la STS implementada.

25.2 Finaliza el procedimiento.

Capítulo 6

Evaluación de la propuesta

Evaluación de la propuesta

La propuesta del caso de estudio se hace en torno al rediseño de toda la red de datos de la Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco. En cuanto a la evaluación del procedimiento plasmado en el capítulo anterior, con sus 3 componentes, se tomó un piso del edificio.

6.1 Descripción del caso de estudio

El edificio, ubicado en Marcelo T. de Alvear 145 de la ciudad de Resistencia-Chaco, forma parte de la estructura de la red metropolitana, de ahí su particular importancia a diferencia de otros edificios de organismos públicos. El mismo está compuesto por 12 pisos, y en cada uno de ellos hay oficinas que pertenecen a más de un organismo. Cuenta con una Sala de Conectividad Principal, en la azotea del edificio, a la cual sólo puede ingresar personal técnico autorizado de la empresa Ecom Chaco S.A.

Dada la particularidad del edificio se contempló la implementación 1 Sala Tecnológica Segura por piso como se muestra en la Figura 27.

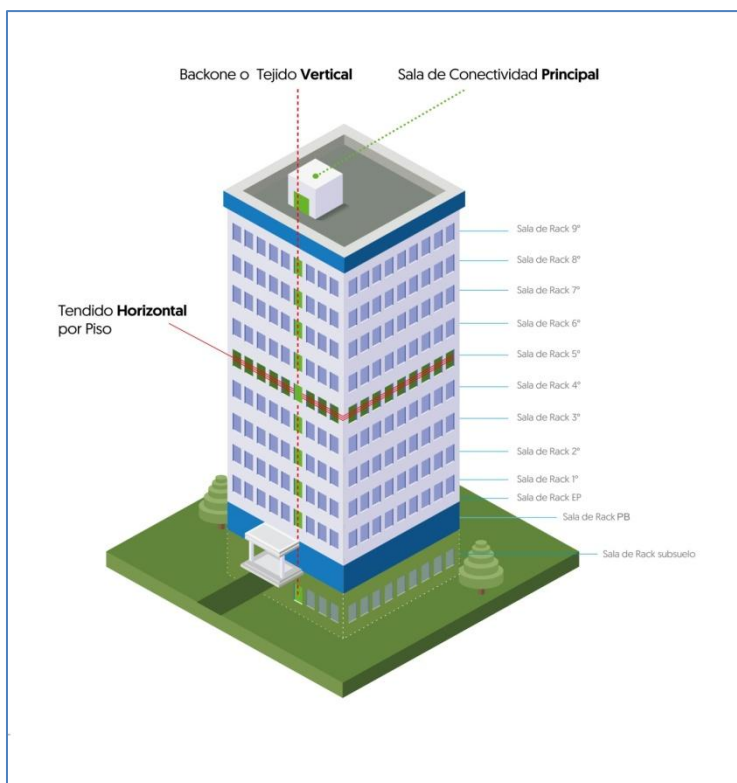


Figura 27: STS en Casa de Gobierno [Elaboración propia]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

El diseño físico para la red de datos del edificio de Casa de Gobierno se puede visualizar en la Figura 28.



Figura 28: Diseño físico red de datos Casa de Gobierno [Elaboración propia]

Para la evaluación del procedimiento propuesto, se tomó de referencia el 5º piso del edificio de Casa de Gobierno, contemplando sus 3 componentes:

1. Componente 1: Informe de la infraestructura tecnológica.
2. Componente 2: Construcción - obra civil de la STS.
3. Componente 3: Adquisición de electrónica y elementos de conectividad para la STS.

Para la toma de datos se diseñó un formulario de relevamiento de la infraestructura tecnológica de los organismos, el cual figura en el ANEXO I, con su correspondiente instructivo que figura en el ANEXO II.

El informe de la infraestructura tecnológica del organismo, junto con la estimación de costos asociada, se encuentra en el Anexo III.

6.2 Estimación de riesgos

De acuerdo al Libro Guía de Técnicas de Magerit V3 [3], se puede realizar una estimación del riesgo haciendo un análisis mediante tablas. Por medio de escalas cualitativas es posible modelar impacto, probabilidad y riesgo.

Tabla 8: Escalas cualitativas [3]

Escalas cualitativas		
impacto	probabilidad	riesgo
MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Así mismo, pueden combinarse impacto y frecuencia (probabilidad) en una tabla, para calcular el riesgo:

Tabla 9: Estimación del riesgo [3]

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Luego del relevamiento de los datos del 5º piso, antes de la elaboración del informe de infraestructura tecnológica del organismo, se efectuó una estimación de riesgos en base a los datos obtenidos y a los riesgos contemplados en la Tabla 7 (riesgos de la infraestructura tecnológica).

La información relevada del 5º piso, se puede observar en la siguiente tabla.

Tabla 10: Datos relevados 5º piso Casa de Gobierno [Elaboración propia]

DATOS GENERALES	
Fecha	14/07/2021
Organismo	Instituto de Colonización
Responsable Informático	
DNI	35030575

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Apellido y Nombre	Toffaletti, Guillermo Joel
Teléfono	4448000 - Interno 8486
E-mail	guille.toffa@gmail.com
Oficina	Unidad de Planificación Sectorial
Observaciones	
SERVIDORES	
Posee Servidores?	SI
Virtual	2
Físico	1
¿Quién los administra?	Personal Interno
¿Todos los servidores cuentan con UPS?	NO
Cantidad de Servidores	
Tower	1
Rackeables	0
Indicar cuantos servidores X86 posee	1
Indicar cantidad de acuerdo a la marca	
Clones / PC Genérica	1
IBM	
HP	
Dell	
Cisco	
Otros	
Indicar la cantidad según Sistema Operativo instalado	
Windows XP	
Windows 2000	
Windows 98	
Windows 2003	
Windows 2008	
Windows 2012	
Linux	3
Unix	
Otro	
¿Los servidores cuentan con respaldo de datos?	SI
En caso de contar con respaldo, especificar el medio	Discos rígidos
Indicar como se ejecuta el respaldo y archivado	Automáticamente
¿Cuenta con archivado fuera de sitio?	NO
Observaciones	
CUARTOS DE EQUIPOS/COMUNICACIONES	
¿Cuenta con una habitación exclusiva para servidores y/o equipos de comunicaciones?	NO
¿La habitación se encuentra refrigerada?	
¿Cuenta con línea eléctrica independiente?	
¿La habitación cuenta con algún mecanismo de seguridad de acceso?	
¿La habitación cuenta con sensores?	

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Observaciones	
RED INTERNA	
¿Quién la administra?	Ecom Chaco S.A., Personal Interno
¿Cuenta con Firewall?	NO
Si cuenta con Firewall ¿de qué marca es?	
El acceso a internet ¿por quién es provisto?	ECOM Chaco S.A.
¿Posee Switches?	SI
De los Switches especificar cantidad	
Administrables	3
Estándares	3
¿Todos los Switches se encuentran instalados en Racks?	SI
¿El rack principal o central cuenta con línea eléctrica independiente?	NO
¿El cableado de red se distribuye a través de bandejas?	NO
Estado general del cableado del organismo	Malo
Los dispositivos de conectividad cuentan con protección energética (UPS)	NO
Cuenta con un diagrama actualizado de la red	NO
Observaciones	

6.2.1 Servidores sin respaldo de datos

Del relevamiento surgió que los servidores del organismo cuentan con respaldo de datos en discos rígidos, realizados de manera automática.

El riesgo es crítico al exponer los servidores sin un medio de respaldo de datos, pero al implementar alguna salvaguarda de backup, el riesgo disminuye y se convierte en apreciable. Se puede estimar que el impacto sería medio, ya que tienen implementado resguardo de datos en discos rígidos, y en el caso de fallas no se perderían los mismos. Así mismo la probabilidad de ocurrencia de pérdida de datos es posible, si no tuvieran respaldo de datos de los servidores del organismo.

Tabla 11: Riesgo servidores sin respaldo de datos [Elaboración propia]

Riesgo		Probabilidad				
		MB	B	M	A	MA
Servidores sin respaldo de datos						
Impacto	MA					
	A					
	M			M		
	B					
	MB					

6.2.2 Los servidores no cuentan con una protección energética (UPS)

Del relevamiento surgió que los servidores del organismo no cuentan con UPS.

El riesgo es importante si los servidores del organismo no cuentan con UPS. Se puede estimar que el impacto sería alto, en el caso que los equipos no posean ups en su mayoría, quedando expuestos a fallas o pudiendo llegar a quemar los mismos. Así mismo la probabilidad de ocurrencia que se quemen servidores del organismo por no disponer de ups es poco probable.

Tabla 12: Riesgo los servidores no cuentan con UPS [Elaboración propia]

Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A		A			
	M					
	B					
	MB					

6.2.3 Espacio físico no delimitado

Del relevamiento surgió que el organismo no cuenta con habitación exclusiva para servidores y/o equipos de comunicaciones.

En la estimación del riesgo que el organismo no cuente con una habitación exclusiva para los equipos de comunicaciones y servidores, se puede estimar un riesgo crítico, debido a la exposición a daños naturales por fuego, agua, y a daños intencionales. Por lo tanto, el impacto de no contar con un espacio físico seguro puede ser muy alto. Así mismo la probabilidad de ocurrencia de dichos daños naturales o intencionales es posible, ya que han ocurrido hechos significativos.

Tabla 13: Riesgo espacio físico no delimitado [Elaboración propia]

Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					

6.2.4 Conexiones eléctricas deficientes

Del relevamiento surge que el organismo no cuenta con conexión eléctrica independiente para los cuartos de equipos/comunicaciones.

En la estimación del riesgo que el organismo no cuente con conexión eléctrica independiente para los cuartos de equipos/comunicaciones, se puede estimar un riesgo crítico, debido a la exposición a fallas en la alimentación del suministro. Por lo tanto, el impacto de tener conexiones eléctricas deficientes puede ser muy alto. Así mismo la probabilidad de ocurrencia de fallas eléctricas por conexiones deficientes en el organismo, es prácticamente seguro.

Tabla 14: Riesgo conexiones eléctricas deficientes [Elaboración propia]

Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					

6.2.5 Cableado de red no documentado

Del relevamiento surge que el organismo no cuenta con planos de redes, de etiquetados y rotulados, lo cual dificulta la ubicación de bocas en mal estado o fuera de funcionamiento.

En la estimación del riesgo que el organismo no cuente con un cableado de red documentado, se puede estimar un riesgo apreciable. Por lo tanto, el impacto de tener un cableado de red no documentado es bajo. Así mismo la probabilidad de ocurrencia de encontrar bocas en mal estado o fuera de funcionamiento en el organismo, es prácticamente seguro.

Tabla 15: Riesgo cableado de red no documentado [Elaboración propia]

Riesgo		Probabilidad				
Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					

6.2.6 Red no administrada

Del relevamiento surge que el organismo cuenta con personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco SA.

En la estimación del riesgo que el organismo no cuente con personal interno o externo que administre la red, lo cual dificulta la aplicación de políticas de seguridad de la información y su cumplimiento, se puede estimar un riesgo bajo. Por lo tanto, el impacto de no contar con personal interno que administre la red es bajo, ya que se cuenta con personal técnico de Ecom que puede suplir dicha necesidad. Así mismo la probabilidad de no contar con personal interno o externo que cumpla dichas funciones es posible.

Tabla 16: Riesgo red no administrada [Elaboración propia]

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

El resultado del Informe de Infraestructura Tecnológica del 5º Piso de Casa de Gobierno se basa en una estimación de riesgos de los datos relevados.

Tabla 17: Resultado de la estimación de riesgos 5º Piso [Elaboración propia]

Ítem	Riesgo	Estimación del riesgo	Salvaguardas implementadas
1	Servidores sin respaldo de datos	Apreciable	Backup automático en discos rígidos
2	Los servidores no cuentan con una protección energética (UPS)	Importante	Sin salvaguardas
3	Espacio físico no delimitado	Crítico	Sin salvaguardas
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco SA
Resultado de la estimación de riesgos		Negativo	De 6 ítems considerados en el análisis, sólo 2 tienen implementadas salvaguardas, mientras que los 4 restantes no tienen ninguna.

6.3 Discusión de resultados

Para poder plasmar informe de la infraestructura tecnológica de cada piso del edificio, se realizó un relevamiento a través de un formulario de Google, el cual respeta las secciones del formulario de relevamiento de la infraestructura tecnológica de los organismos, que figura en el ANEXO I, y su instructivo que figura en el ANEXO II. Los enlaces al formulario y sus respuestas son:

- Formulario de Relevamiento de Google (acceso público)

<https://docs.google.com/forms/d/1u9DqeZZ1FXZ-ICb1s2LTtxbmWAmXObyZ4OV7fCOMrrE/edit?usp=sharing>

- Respuestas del Relevamiento (acceso público)

<https://docs.google.com/spreadsheets/d/1VDSXS1F9uJrYeS7IN4P8OU7HAhXI9Pj8wYR1jf0r6Fw/edit?usp=sharing>

Luego del relevamiento de los 12 pisos, se plasmó un informe de la infraestructura tecnológica de cada piso, basado en una estimación de riesgos para cada variable de análisis, plasmadas en la Tabla 7 (riesgos de la infraestructura tecnológica).

En la estimación de riesgos de cada piso, se procedió de manera similar a lo descrito en el punto 6.2, donde se ejemplifica como se llevó adelante el análisis en el 5º Piso del edificio.

El resultado del informe de infraestructura tecnológica de cada piso, está asociado a las salvaguardas implementadas para cada uno de los ítems de la Tabla 7, como puede observarse en la Tabla 18. El total de informes negativos y positivos obtenidos, se visualiza en el Gráfico 1.

Tabla 18: Resultados Informe IT por piso del edificio [Elaboración propia]

Informes x Piso	Servidores sin respaldo de datos	Los servidores no cuentan con una protección energética (UPS)	Espacio físico no delimitado	Conexiones eléctricas deficientes	Cableado de red no documentado	Red no administrada	Con salvaguardas	Sin salvaguardas	Ítems No contemplado	Resultado Informe IT
Planta Baja	Backup manual en discos rígidos	UPS	Cuarto de comunicaciones	Línea eléctrica independiente	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.	5	1		Positivo
Subsuelo	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa	1	5		Negativo

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

						Ecom Chaco S.A.				
Entrepiso	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.	1	5		Negativo
1º Piso	No contemplado	No contemplado	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Técnicos de la empresa Ecom Chaco S.A.	1	3	2	Negativo
2º Piso	Sin salvaguardas	UPS	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.	2	4		Negativo
3º Piso	No contemplado	No contemplado	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Técnicos de la empresa Ecom Chaco S.A.	1	3	2	Negativo
4º Piso	Backup manual en discos rígidos	UPS	Cuarto de comunicaciones	Sin salvaguardas	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.	4	2		Positivo
5º Piso	Backup automático en discos rígidos	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.	2	4		Negativo
6º Piso	Sin salvaguardas	Sin salvaguardas	Cuarto de comunicaciones	Sin salvaguardas	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.	2	4		Negativo
7º Piso	Backup manual en discos rígidos	UPS	Cuarto de comunicaciones	Sin salvaguardas	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.	4	2		Positivo
8º Piso	Sin salvaguardas	Sin salvaguardas	Cuarto de comunicaciones	Sin salvaguardas	Sin salvaguardas	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.	2	4		Negativo
9º Piso	Sin salvaguardas	Sin salvaguardas	Cuarto de comunicaciones	Línea eléctrica independiente	Sin salvaguardas	Técnicos de la empresa Ecom Chaco S.A.	3	3		Negativo

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Así podemos expresar lo siguiente:

- Si (ítems con salvaguardas =< ítems sin salvaguardas) => Informe IT Negativo.
- Si (ítems con salvaguardas > ítems sin salvaguardas) => Informe IT Positivo.

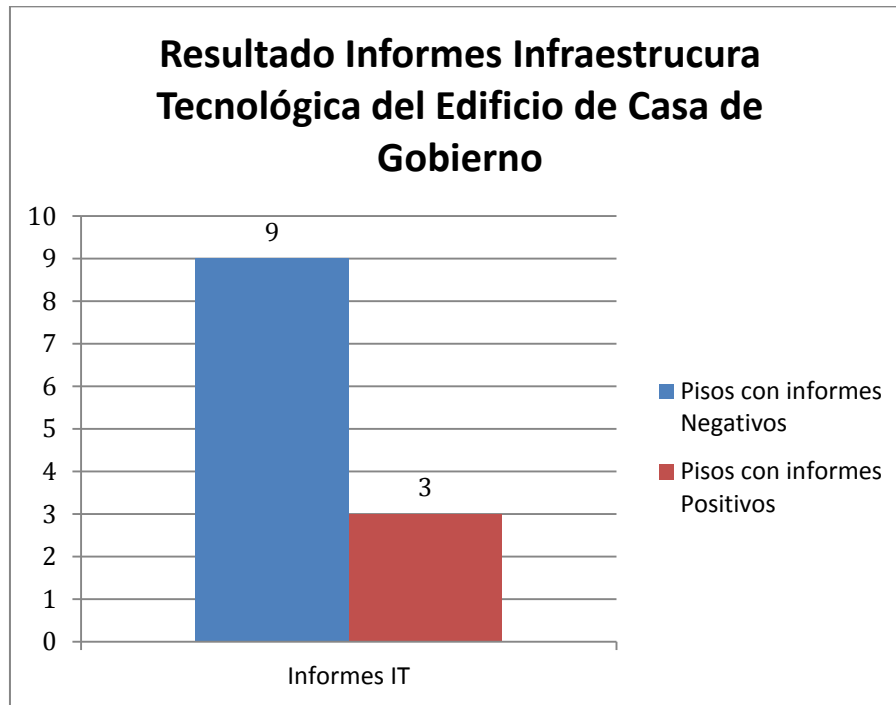


Gráfico 1: Resultado Informes IT del edificio

Las estimaciones de riesgos de los 12 pisos del edificio, se visualizan en la Tabla 19, y los resultados se expresan en porcentajes en los Gráficos 2 a 7.

Tabla 19: Estimaciones de riesgos por piso [Elaboración propia]

Riesgos x Piso	Servidores sin respaldo de datos	Los servidores no cuentan con una protección energética (UPS)	Espacio físico no delimitado	Conexiones eléctricas deficientes	Cableado de red no documentado	Red no administrada
Subsuelo	Crítico	Importante	Crítico	Crítico	Apreciable	Bajo
Planta Baja	Apreciable	Bajo	Apreciable	Apreciable	Apreciable	Bajo
Entrepiso	Crítico	Importante	Crítico	Crítico	Apreciable	Bajo
1º Piso	Despreciable	Despreciable	Crítico	Crítico	Apreciable	Bajo
2º Piso	Crítico	Bajo	Crítico	Crítico	Apreciable	Bajo
3º Piso	Despreciable	Despreciable	Crítico	Crítico	Apreciable	Bajo
4º Piso	Apreciable	Bajo	Apreciable	Crítico	Apreciable	Bajo
5º Piso	Apreciable	Importante	Crítico	Crítico	Apreciable	Bajo
6º Piso	Crítico	Importante	Apreciable	Crítico	Apreciable	Bajo

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

7ºPiso	Apreciable	Bajo	Apreciable	Crítico	Apreciable	Bajo
8ºPiso	Crítico	Importante	Apreciable	Crítico	Apreciable	Bajo
9ºPiso	Crítico	Importante	Apreciable	Apreciable	Apreciable	Bajo
Resultados						
Crítico	6	0	6	10	0	0
Importante	0	6	0	0	0	0
Apreciable	4	0	6	2	12	0
Bajo	0	4	0	0	0	12
Despreciable	2	2	0	0	0	0
Total	12	12	12	12	12	12

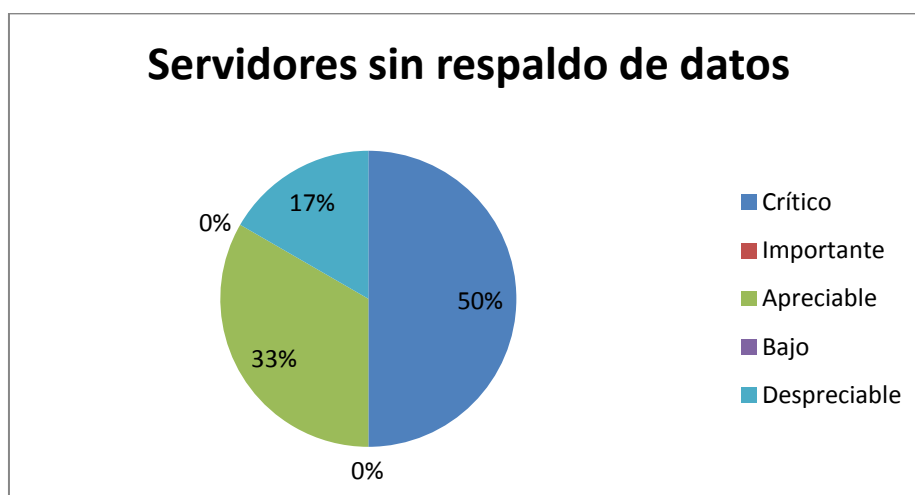


Gráfico 2: Riesgo servidores sin respaldo de datos

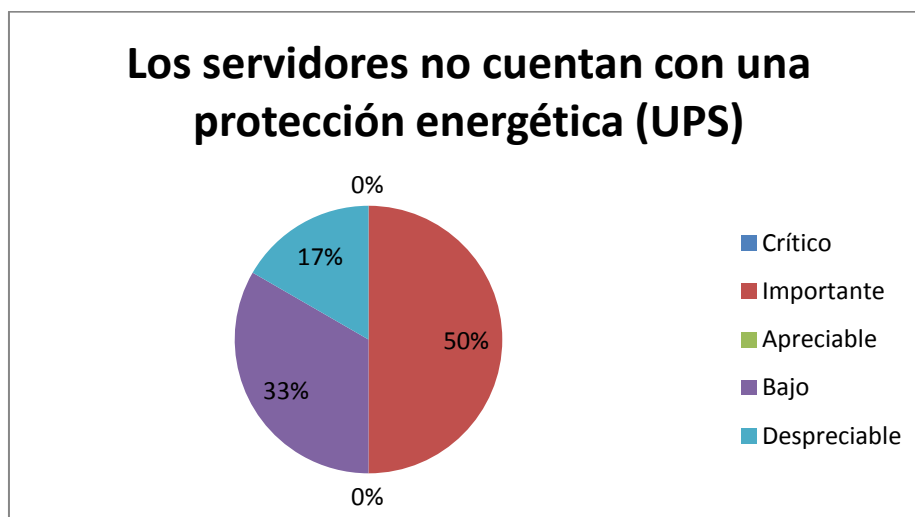


Gráfico 3: Riesgo los servidores no cuentan con una protección energética (UPS)

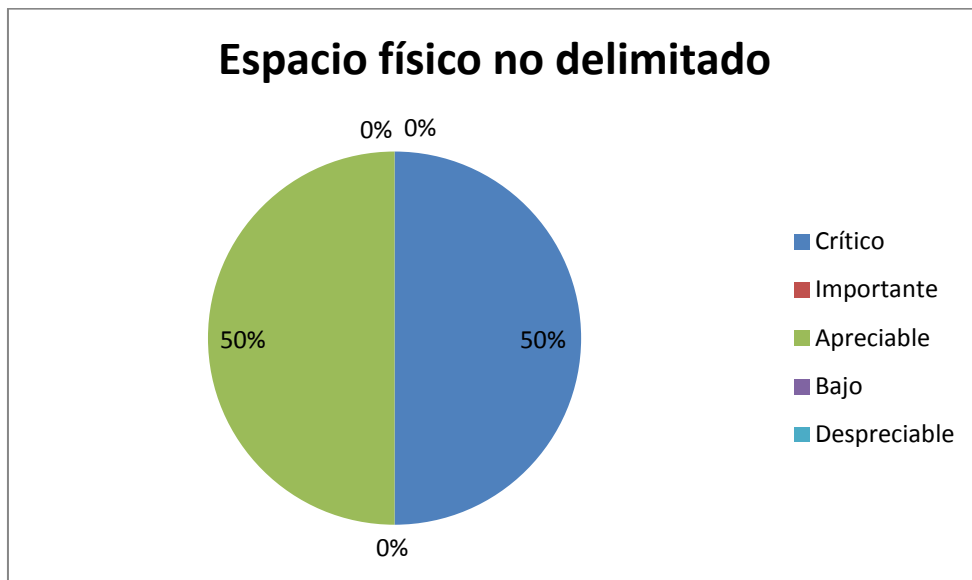


Gráfico 4: Riesgo espacio físico no delimitado

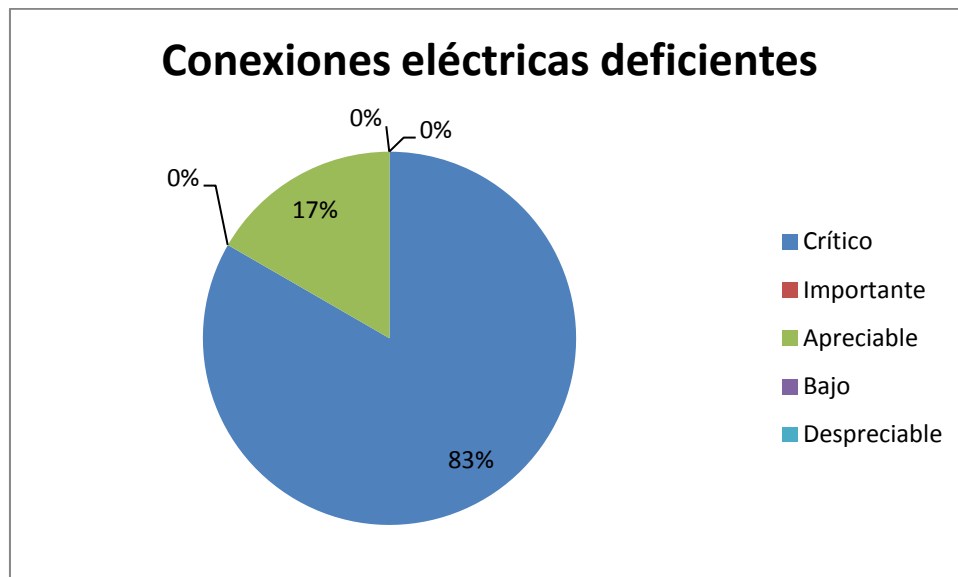


Gráfico 5: Riesgo conexiones eléctricas deficientes

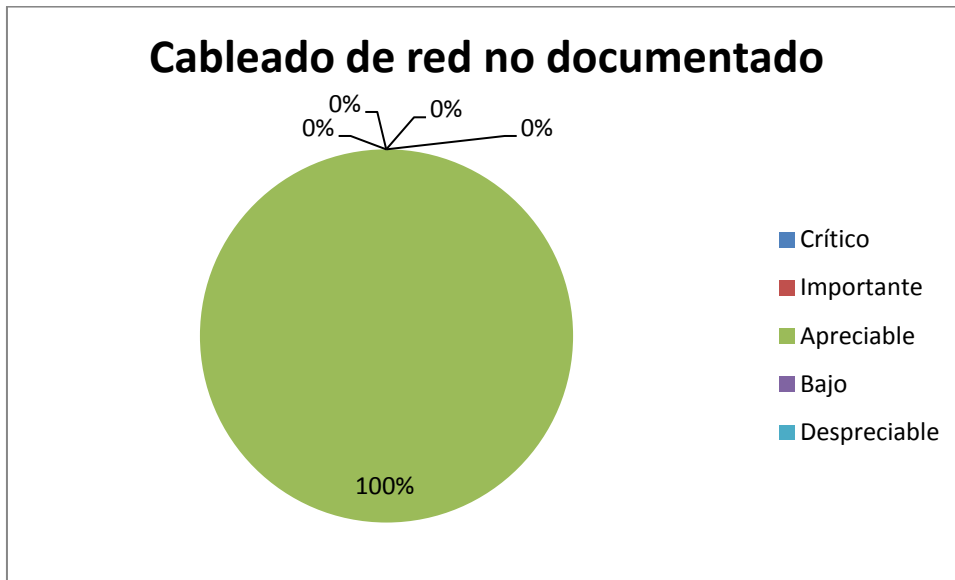


Gráfico 6: Riesgo cableado de red no documentado

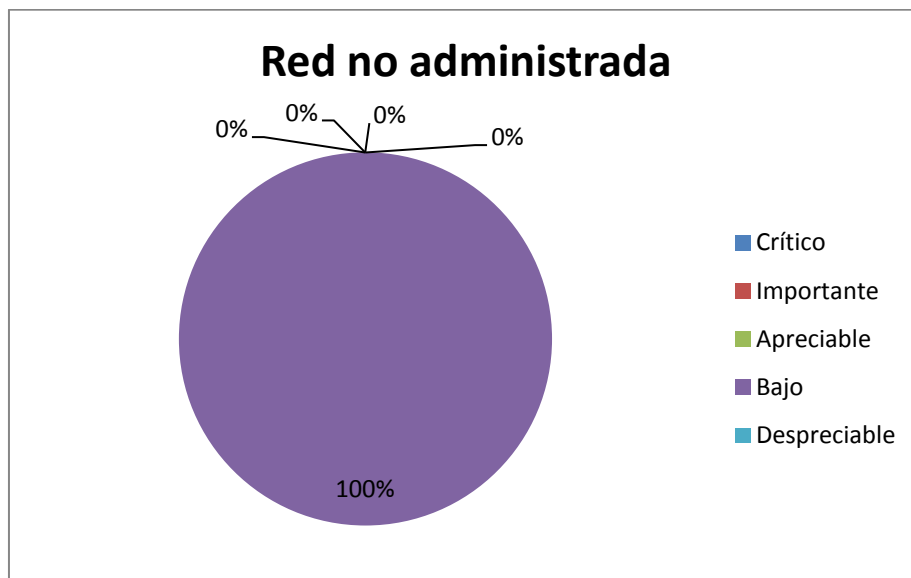


Gráfico 7: Riesgo red no administrada

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

En cuanto a las salvaguardas implementadas, se contabilizan las mismas, como también las no implementadas y las no contempladas.

Tabla 20: Salvaguardas por riesgo [Elaboración propia]

Salvaguardas por riesgo	Servidores sin respaldo de datos	Los servidores no cuentan con una protección energética (UPS)	Espacio físico no delimitado	Conexiones eléctricas deficientes	Cableado de red no documentado	Red no administrada
No contemplado	2	2				
Sin salvaguardas	6	6	6	10	12	
Backup manual en discos rígidos	3					
Backup automático en discos rígidos	1					
UPS		4				
Cuarto de comunicaciones			6			
Línea eléctrica independiente				2		
Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.						9
Técnicos de la empresa Ecom Chaco S.A.						3

En el caso de los pisos que cuentan con un cuarto de comunicaciones, que de acuerdo a la Tabla 18 son 6 pisos (Planta Baja, 4º, 6º, 7º, 8º y 9º), se recomendó la mejora de los mismos, convirtiendo éstos en Salas Tecnológicas Seguras, que contemplen los requerimientos de seguridad física y ambiental para el alojamiento de los equipos y recursos de conectividad.

En el caso de los pisos que no cuentan con un cuarto de comunicaciones, que de acuerdo a la Tabla 18 son 6 pisos (Subsuelo, Entrepiso, 1º, 2º, 3º, 5º), se propone la construcción de Salas Tecnológicas Seguras, ya que no disponen de habitaciones exclusivas para servidores y/o equipos de comunicaciones.

6.3.1 Análisis de los resultados obtenidos de los organismos del caso de estudio

En la Tabla 18, se observa que, de los 12 pisos del edificio, 9 de ellos dieron como resultado un informe de IT negativo, lo cual fundamenta el pedido de construcción e implementación de la STS en los pisos. A diferencia de tres pisos (4º Piso, 7º Piso y Planta Baja del edificio), que dieron como resultado del informe de IT positivo, lo cual no fundamenta el pedido de construcción e implementación de STS.

Aquí podemos detenernos para analizar lo siguiente, el procedimiento propuesto plasma que para iniciar el pedido de construcción de la STS, el informe de infraestructura tecnológica del organismo debe ser negativo, es decir deberían ser negativos para los 12 pisos, pero como el caso de estudio está enmarcado en el proyecto de "Rediseño, saneamiento y adecuación de la red de datos del edificio de Casa de Gobierno", aprobado por Resolución Nº 2515/2017 de la Secretaría General de Gobernación [35], se incluyen los tres pisos (4º Piso, 7º Piso y Planta Baja del edificio), para la implementación de las STS.

6.3.2 Organismos que no están contemplados en el caso de estudio

Ahora si aplicamos el procedimiento a otros organismos públicos, fuera del edificio de Casa de Gobierno, que no están incluidos en el proyecto antes mencionado, pueden presentarse dos situaciones:

- a. Análisis de situación 1: Si uno de estos organismos quiere implementar una STS, el mismo no podrá iniciar el pedido de implementación de STS, si el informe de infraestructura tecnológica del mismo resulta positivo, debido a razones atadas a lo presupuestario.
- b. Análisis de situación 2: Si uno de estos organismos quiere implementar una STS, y el informe de infraestructura tecnológica del mismo resulta positivo, lo cual no fundamenta la construcción de la STS; el mismo podrá solicitar la construcción de una STS, siempre y cuando exista un proyecto marco que avale la solicitud de implementación de una STS, tal cual lo planteado en el caso de estudio.

Para ejemplificar lo planteado, partimos del Informe de la Infraestructura Tecnológica del organismo Dirección de Catastro y Cartografía de la Provincia del Chaco, el cual se encuentra fuera del edificio de Casa de Gobierno. Éste organismo, está bastante organizado y ordenado

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

en cuanto a su infraestructura, por lo cual el resultado de la estimación de los riesgos contemplados en la Tabla 7 resultó positivo; por lo tanto, no se tiene fundamento para pedir la implementación de una STS en dicho organismo.

Por tal motivo se incluyó la implementación de una STS en el proyecto de "Fortalecimiento, integración e interoperabilidad de la Dirección de Catastro y Cartografía, Registro de la Propiedad Inmueble y la Administración Tributaria Provincial", el cual se gestiona en el marco del Programa de Fortalecimiento de la Gestión Provincial BID 4753 OC/AR.

En nación la entidad responsable ante el BID es:

- Ministerio del Interior de la Nación / Secretaría de Provincias
- Dirección de Análisis Seguimiento y Evaluación de Programas de Desarrollo regional (DASEPR)

En la Provincia del Chaco el organismo coordinador es la:

- Subsecretaría de Modernización del Estado, dependiente de la Secretaría General de Gobernación.

Los organismos provinciales beneficiarios del proyecto son:

- Ministerio de Gobierno y Trabajo
 - Dirección Provincial de Catastro y Cartografía
 - Dirección General del Registro de la Propiedad Inmueble
- Administración Tributaria Provincial (ATP)

6.3.3 Estimación de costos

En cuanto a los costos proyectados para 12 STS con 4000 puestos de trabajo en el edificio de Casa de Gobierno, tomamos de referencia la estimación del 5º Piso plasmada en del ANEXO III.

Tabla 21: Estimación de costos STS [Elaboración propia]

Agrupación	Ítems	USD Dólares
SCE	Elementos de cableado estructurado dentro de la Sala Segura	\$5.737,04
	Elementos de cableado estructurado despliegue horizontal	\$12.276,70
STS	Equipamiento TIC Sala Segura	\$7.839,74
	Obra Civil Sala Segura	\$6.852,52
	Sistema de Videovigilancia	\$2.696,68
	SCE	\$18.013,74
	STS	\$17.388,94
	Total STS + SCE	\$35.402,68

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Para calcular el costo de instalación de 1 puesto de red, nos basamos en los 117 de puestos estimados en el ANEXO III, con lo cual obtenemos que:

- $SCE \$ 18.013,74 / 117 \text{ puestos} = \$ 153,96 \text{ (USD)}$.

En base al dato del costo de instalación de un puesto, podemos proyectar el mismo para 4000 puestos de red, haciendo el cálculo de:

- $\$ 153,96 * 4000 = \$ 615.840,00 \text{ (USD)}$

Tabla 22: Estimación para 4000 puestos de red [Elaboración propia]

Costo de instalación de un puesto de red, desde la STS del piso hasta el puesto de trabajo.	\$ 153,96
Cantidad de puestos de trabajo en el edificio de Casa de Gobierno	4000
Costo de instalación de 4000 puestos de red, desde las STS de los pisos hasta los puestos de trabajo	\$ 615.840,00

En base a los datos de los costos estimados de 1 STS, podemos proyectar el mismo para 12 STS, para todo el edificio de Casa de Gobierno, como se visualiza en la Tabla 23, haciendo el cálculo de:

- $\$ 17.388,94 * 12 = \$ 208.667,28 \text{ (USD)}$.

Tabla 23: Estimación para 12 STS [Elaboración propia]

Id	Piso	STS
1	Subsuelo	\$17.388,94
2	Planta Baja	\$17.388,94
3	Entrepiso	\$17.388,94
4	1º Piso	\$17.388,94
5	2º Piso	\$17.388,94
6	3º Piso	\$17.388,94
7	4º Piso	\$17.388,94
8	5º Piso	\$17.388,94
9	6º Piso	\$17.388,94
10	7ºPiso	\$17.388,94
11	8ºPiso	\$17.388,94
12	9ºPiso	\$17.388,94
Total		\$208.667,28

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Con lo cual podemos concluir que el costo proyectado para las 12 STS y 4000 puestos de red es de \$ 824.507,28 (USD).

Tabla 24: Estimación total de costos para el proyecto [Elaboración propia]

	USD (Dólares)
12 STS	\$ 208.667,28
4000 puestos de red del SCE	\$ 615.840,00
Estimación de costos para el proyecto	\$ 824.507,28

Capítulo 7

Conclusiones y futuras líneas de trabajo

Conclusiones y futuras líneas de trabajo

El presente Trabajo Final de Maestría, ha permitido encontrar solución a las necesidades planteadas como problemas en el capítulo 3:

1. Problemas en la aplicación de estándares de la industria en materia telecomunicaciones.
2. Falta de propuestas que permitan plasmar políticas, que contemplen inversiones en materia de infraestructura tecnológica robusta, conectividad y seguridad de la información.

En el primer punto incorporando al Sistema de Cableado Estructurado (SCE) de los organismos públicos, un modelo de "Sala Tecnológica Segura", como espacio físico en los edificios, destinado a concentrar los dispositivos principales de la infraestructura tecnológica, que necesitan ser protegidos para su correcto funcionamiento; el cual incorpora características de los cuartos de equipos, los cuartos de telecomunicaciones y datacenters, basados en los estándares de la industria ANSI/TIA 568, 569 y 942.

En el segundo punto incorporando el modelo de "Sala Tecnológica Segura", mediante un procedimiento que permite analizar la infraestructura tecnológica de los organismos públicos, y en base a una estimación de riesgos, fundamentar el pedido de inversión para la construcción e implementación de las salas.

Es importante resaltar como logro, la firma del primer decreto con firma digital del gobernador, Decreto Nº 483/2022 [51], el cual crea el fideicomiso denominado "Fideicomiso de Modernización del Estado", por el cual se canalizarán las erogaciones presupuestarias que demanden las mejoras de la red de datos de los organismos públicos, que resulten de la aplicación del procedimiento propuesto.

Otro ítem a resaltar, es el trabajo conjunto que se lleva adelante entre áreas competentes del Poder Ejecutivo, para lograr la instrumentación legal en el marco del decreto mencionado en el párrafo anterior, de la propuesta técnica (Capítulo 4), su procedimiento de implementación (Capítulo 5), y políticas de seguridad de la información (Anexo IV). Puesto

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

que el mismo brindará a la Administración Pública Provincial del Poder Ejecutivo del Chaco, de una herramienta para la gobernanza de las telecomunicaciones, que promoverá el desarrollo de una infraestructura tecnológica y conectividad homogénea en los organismos públicos.

La investigación cualitativa nos llevó a plantear la hipótesis, que los organismos de la Administración Pública Provincial del Chaco, más avanzados en la implementación de los nuevos procesos y procedimientos de base digital, son los que tienen una adecuada organización de sus recursos humanos, su infraestructura tecnológica y conectividad.

Lo mencionado anteriormente, se evidencia en las similitudes y diferencias de la organización interna de los organismos de Casa de Gobierno, ya que los más retrasados en pasar de trámites en formato papel a trámites en formato electrónico, distan de tener una eficiente infraestructura tecnológica y conectividad, que soporte los nuevos procesos de transformación digital.

7.1 Contribuciones del trabajo

La principal contribución del trabajo de maestría profesional, es la aplicación práctica en:

1. Los organismos públicos contemplados en el caso de estudio.

Por medio de la inclusión del modelo de Sala Tecnológica Segura (STS), con su correspondiente procedimiento de implementación, el cual también aplica a los organismos públicos no contemplados en el caso de estudio.

2. Los proyectos de inversión, que buscan mejorar la conectividad de los organismos.

Los proyectos gestionados ante el Banco Interamericano de Desarrollo (BID), o ante el Fondo de Garantía de Sustentabilidad (FGS) de ANSES, que contemplan en sus líneas de financiamiento la adquisición de bienes de capital, obras civiles y mejoras edilicias.

3. El Ecosistema de Integrabilidad Digital del Chaco - EDICH.

La provincia ha comenzado a recorrer el camino para la implementación de un ecosistema digital de integrabilidad, con despliegue en el Poder Ejecutivo y capacidad de expansión hacia los otros Poderes del Estado, como así también el sector privado, que permita garantizar la integridad, seguridad, confianza y no repudio en el intercambio de datos, procesos y servicios digitales. Para ello se basa en la

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

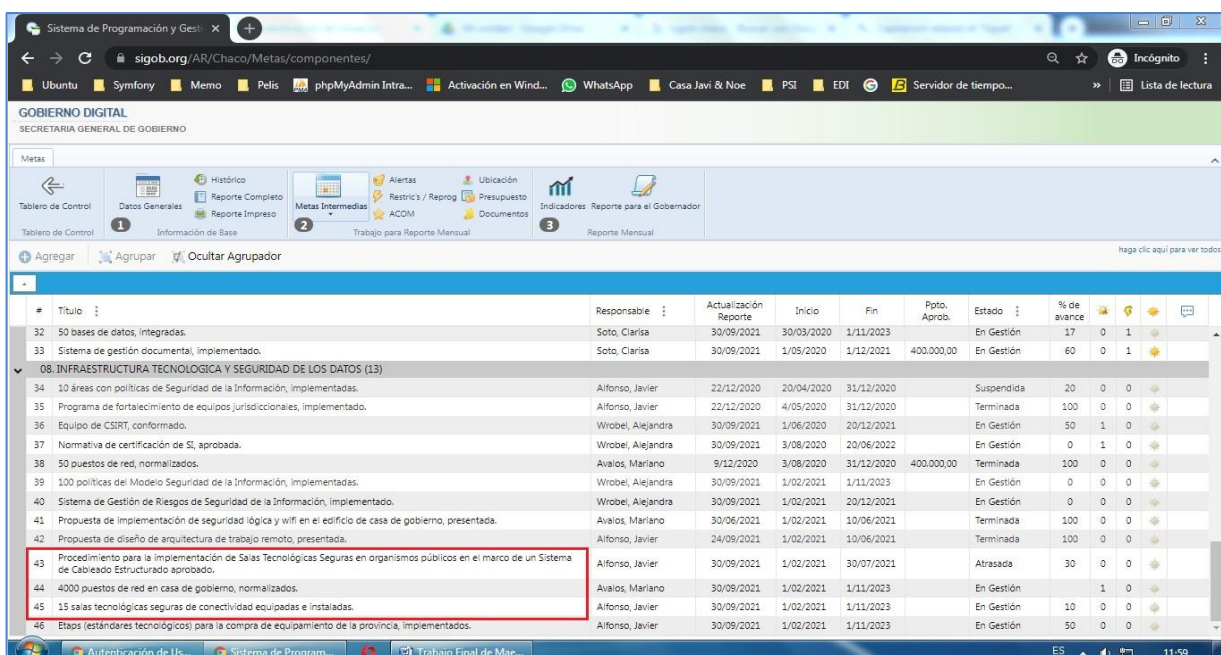
arquitectura distribuida peer to peer (punto a punto) de servidores de seguridad X-ROAD [52]. En éste sentido el aporte de las Salas Tecnológicas Seguras (STS) al ecosistema, es brindar un espacio físico seguro para el alojamiento de éstos servidores, en los organismos públicos identificados como fuentes auténticas de datos.

4. Las metas de gobierno de la Provincia del Chaco.

Las metas plasmadas en el presupuesto 2022, contemplan la mejora de la conectividad y seguridad de la información de los organismos y dependencias del estado provincial; invirtiendo en una infraestructura tecnológica robusta, que implementa Salas Tecnológicas Seguras, como parte de los sistemas de cableado de telecomunicaciones.

En esta última contribución se resalta, que la provincia ha implementado para mejorar la eficacia de las políticas públicas, el Sistema de Gestión para la Gobernabilidad (SIGOB), del Programa de Naciones Unidas para el Desarrollo (PNUD) [53][54].

El Sistema de Metas de la Gobernación del Chaco basado en el SIGOB, contempla la implementación del procedimiento propuesto, los puestos de red normalizados y las salas tecnológicas seguras, como se visualiza en las metas intermedias 43, 44 y 45 de la Figura 29.



#	Título	Responsable	Actualización Reporte	Inicio	Fin	Ppto. Aprob.	Estado	% de avance	👍	👎	👉	🗨️
32	50 bases de datos, integradas.	Soto, Clarisa	30/09/2021	30/03/2020	1/11/2023		En Gestión	17	0	1	👉	
33	Sistema de gestión documental, implementado.	Soto, Clarisa	30/09/2021	1/05/2020	1/12/2021	400.000,00	En Gestión	60	0	1	👉	
08. INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD DE LOS DATOS (13)												
34	10 áreas con políticas de Seguridad de la Información, implementadas.	Alfonso, Javier	22/12/2020	20/04/2020	31/12/2020		Suspendida	20	0	0	👉	
35	Programa de fortalecimiento de equipos jurisdiccionales, implementado.	Alfonso, Javier	22/12/2020	4/05/2020	31/12/2020		Terminada	100	0	0	👉	
36	Equipo de CSIRT, conformado.	Wrobel, Alejandra	30/09/2021	1/06/2020	20/12/2021		En Gestión	50	1	0	👉	
37	Normativa de certificación de SI, aprobada.	Wrobel, Alejandra	30/09/2021	3/08/2020	20/06/2022		En Gestión	0	1	0	👉	
38	50 puestos de red, normalizados.	Avalos, Mariano	9/12/2020	3/08/2020	31/12/2020	400.000,00	Terminada	100	0	0	👉	
39	100 políticas del Modelo Seguridad de la Información, implementadas.	Wrobel, Alejandra	30/09/2021	1/02/2021	1/11/2023		En Gestión	0	0	0	👉	
40	Sistema de Gestión de Riesgos de Seguridad de la Información, implementado.	Wrobel, Alejandra	30/09/2021	1/02/2021	20/12/2021		En Gestión	0	0	0	👉	
41	Propuesta de implementación de seguridad lógica y wifi en el edificio de casa de gobierno, presentada.	Avalos, Mariano	30/06/2021	1/02/2021	10/06/2021		Terminada	100	0	0	👉	
42	Propuesta de diseño de arquitectura de trabajo remoto, presentada.	Alfonso, Javier	24/09/2021	1/02/2021	10/06/2021		Terminada	100	0	0	👉	
43	Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado aprobado.	Alfonso, Javier	30/09/2021	1/02/2021	30/07/2021		Atrasada	30	0	0	👉	
44	4000 puestos de red en casa de gobierno, normalizados.	Avalos, Mariano	30/09/2021	1/02/2021	1/11/2023		En Gestión	1	0	0	👉	
45	15 salas tecnológicas seguras de conectividad equipadas e instaladas.	Alfonso, Javier	30/09/2021	1/02/2021	1/11/2023		En Gestión	10	0	0	👉	
46	Etapos (estándares tecnológicos) para la compra de equipamiento de la provincia, implementados.	Alfonso, Javier	30/09/2021	1/02/2021	1/11/2023		En Gestión	50	0	0	👉	

Figura 29: Metas intermedias 43, 44 y 45 -SIGOB [55]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

7.2 Futuras líneas de trabajo

Dentro de las futuras líneas de trabajo planteamos trabajar en:

1. Un procedimiento para auditar la seguridad física y ambiental de las Salas Tecnológicas Seguras implementadas en los organismos. El cual otorgue certificaciones de seguridad de acuerdo a niveles.
2. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en los organismos públicos, el cual incluya las Políticas de Seguridad de la Información contempladas en el Anexo IV.
3. Desarrollar una plataforma, que permita a los organismos hacer el seguimiento de su Sistema de Gestión de Seguridad de la Información.

El desarrollo de ésta plataforma, se visualiza en la meta intermedia 40 de la Figura 30.

#	Título	Responsable	Actualización Reporte	Inicio	Fin	Ppto. Aprob.	Estado	% de avance	👍	👎	🔔	
32	50 bases de datos, integradas.	Soto, Clarisa	30/09/2021	30/03/2020	1/11/2023		En Gestión	17	0	1	🔔	
33	Sistema de gestión documental, implementado.	Soto, Clarisa	30/09/2021	1/05/2020	1/12/2021	400.000,00	En Gestión	60	0	1	🔔	
08. INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD DE LOS DATOS (13)												
34	10 áreas con políticas de Seguridad de la Información, implementadas.	Alfonso, Javier	22/12/2020	20/04/2020	31/12/2020		Suspendida	20	0	0	🔔	
35	Programa de fortalecimiento de equipos jurisdiccionales, implementado.	Alfonso, Javier	22/12/2020	4/05/2020	31/12/2020		Terminada	100	0	0	🔔	
36	Equipo de CSIRT, conformado.	Wrobel, Alejandra	30/09/2021	1/06/2020	20/12/2021		En Gestión	50	1	0	🔔	
37	Normativa de certificación de SI, aprobada.	Wrobel, Alejandra	30/09/2021	3/08/2020	20/06/2022		En Gestión	0	1	0	🔔	
38	50 puestos de red, normalizados.	Avalos, Mariano	9/12/2020	3/08/2020	31/12/2020	400.000,00	Terminada	100	0	0	🔔	
39	100 políticas del Modelo Seguridad de la Información, implementadas.	Wrobel, Alejandra	30/09/2021	1/02/2021	1/11/2023		En Gestión	0	0	0	🔔	
40	Sistema de Gestión de Riesgos de Seguridad de la Información implementado.	Wrobel, Alejandra	30/09/2021	1/02/2021	20/12/2021		En Gestión	0	0	0	🔔	
41	Propuesta de implementación de seguridad lógica y wifi en el edificio de casa de gobierno, presentada.	Avalos, Mariano	30/06/2021	1/02/2021	10/06/2021		Terminada	100	0	0	🔔	
42	Propuesta de diseño de arquitectura de trabajo remoto, presentada.	Alfonso, Javier	24/09/2021	1/02/2021	10/06/2021		Terminada	100	0	0	🔔	
43	Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado aprobado.	Alfonso, Javier	30/09/2021	1/02/2021	30/07/2021		Atrasada	30	0	0	🔔	
44	4000 puestos de red en casa de gobierno, normalizados.	Avalos, Mariano	30/09/2021	1/02/2021	1/11/2023		En Gestión	1	0	0	🔔	
45	15 salas tecnológicas seguras de conectividad equipadas e instaladas.	Alfonso, Javier	30/09/2021	1/02/2021	1/11/2023		En Gestión	10	0	0	🔔	
46	Etapas (estándares tecnológicos) para la compra de equipamiento de la provincia, implementados.	Alfonso, Javier	30/09/2021	1/02/2021	1/11/2023		En Gestión	50	0	0	🔔	

Figura 30: Meta intermedia 40 - SIGOB [55]

7.3 Avances del proyecto

En cuanto a los avances del proyecto, podemos citar las siguientes acciones:

- Se relevaron los 12 pisos del edificio de Casa de Gobierno.
- Se construyó la STS del 5º Piso de Casa de Gobierno, se instalaron en una primera etapa 117 puestos de trabajo, con cableado estructurado normalizado en categoría 6,

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

y en una segunda etapa 203, lo cual hace un total de 320 puestos, con nuevo cableado en categoría 6.

- El proyecto de remodelación integral del 5º Piso, se tomó como caso de éxito, ya que sin tener el procedimiento propuesto para la implementación de STS aprobado por instrumento legal correspondiente, se avanzó siguiendo las etapas y pasos del mismo.
- El día 12/04/22, se presentó el procedimiento para la implementación de STS en organismos públicos a los referentes jurisdiccionales, poniendo en conocimiento que se trabaja en un proyecto de decreto, para la instrumentación legal de:
 1. ANEXO I: Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos.
 - a. Relevamiento e informe correspondiente
 - b. Proyecto de mejora de cableado estructurado y wi-fi
 2. ANEXO II: Especificaciones técnicas para las redes de datos.
 - a. Redes inalámbricas
 - b. Cableado horizontal
 - c. Salas tecnológicas seguras
 3. ANEXO III: Políticas de Seguridad de la Información en Salas Tecnológicas Seguras.
 - a. Gestión de Activos
 - b. Control de Accesos
 - c. Seguridad Física y Ambiental
 - d. Seguridad en las Telecomunicaciones
- Una vez aprobado el procedimiento para la implementación de STS en organismos públicos, se consensuó en trabajar con los referentes informáticos designados formalmente, en los proyectos de mejora de las redes de datos de cada piso, contemplando las particularidades de cada organismo por piso.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Referencias

Referencias

- [1] *Cableado genérico de telecomunicaciones para instalaciones de clientes*, TIA-568.0, Revisión E, Marzo, 2020 [En línea]. Disponible en: <https://global.ihs.com/>. [Accedido: 11-Abril-2022]
- [2] Asociación de Industrias de Telecomunicaciones, "TIA", 2022 [En línea]. Disponible en: <https://tiaonline.org/>. [Accedido 11-Abril-2022]
- [3] Ministerio de Hacienda y Administraciones Públicas, *MAGERIT V3 - Libro III - Guía de Técnicas*, España: Universidad Politécnica de Madrid, 2012 [En línea]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Accedido: 11-Abril-2022]
- [4] Organización Internacional para la Estandarización, "ISO", 2022 [En línea]. Disponible en: <https://www.iso.org/home.html>. [Accedido: 11-Abril-2022]
- [5] Comisión Electrotécnica Internacional, "IEC", 2022 [En línea]. Disponible en: <https://www.iec.ch/>. [Accedido: 11-Abril-2022]
- [6] Instituto Americano Nacional de Estándares, "ANSI", 2022 [En línea]. Disponible en: <https://www.ansi.org/>. [Accedido: 11-Abril-2022]
- [7] Asociación de la Industria de Componentes Electrónicos, "ECIA - Conectar. Influcidar. Optimizar", 2022 [En línea]. Disponible en: <https://www.ecianow.org/>. [Accedido: 11-Abril-2022]
- [8] Instituto de Ingenieros Eléctricos y Electrónicos, "IEEE - La organización profesional técnica más grande del mundo para el avance de la tecnología", 2022 [En línea]. Disponible en: <https://www.ieee.org/>. [Accedido: 11-Abril-2022]
- [9] Comité Europeo para la Estandarización Electrotécnica, "CENELEC – Estándares para Europa", 2022 [En línea]. Disponible en: <https://www.cencenelec.eu/>. [Accedido: 11-Abril-2022]
- [10] Instituto Argentino de Normalización y Certificación, "IRAM", 2022 [En línea]. Disponible en: <http://www.iram.org.ar/>. [Accedido: 11-Abril-2022]
- [11] Comisión Panamericana de Normas Técnicas, "COPANT", 2022 [En línea]. Disponible en: <https://www.copant.org/>. [Accedido: 11-Abril-2022]
- [12] Asociación Mercosur de Normalización, "AMN", 2022 [En línea]. Disponible en:

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

<https://www.amn.org.br/>. [Accedido: 11-Abril-2022]

- [13] Comité de Ingeniería TR-42 de la Asociación de la Industria de las Telecomunicaciones (TIA), "TR-42 - Sistemas de cableado de telecomunicaciones", 2022 [En línea]. Disponible en: <http://standards.tiaonline.org/all-standards/committees/tr-42>. [Accedido: 11-Abril-2022]
- [14] *Cableado genérico de telecomunicaciones para instalaciones de clientes*, TIA/EIA-568, Revisión A, Octubre, 1995 [En línea]. Disponible en: <https://global.ihs.com/>. [Accedido: 11-Abril-2022].
- [15] "RJ-45 TIA-568A", *Wikipedia*, 2005 [En línea]. Disponible en: https://es.m.wikipedia.org/wiki/Archivo:RJ-45_TIA-568A_Right.png. [Accedido: 11-Abril-2022]
- [16] *Cableado genérico de telecomunicaciones para instalaciones de clientes*, TIA/EIA-568, Revisión B, Abril, 2001 [En línea]. Disponible en: <https://global.ihs.com/>. [Accedido: 11-Abril-2022]
- [17] "RJ-45 TIA-568B", *Wikipedia*, 2005 [En línea]. Disponible en: https://es.m.wikipedia.org/wiki/Archivo:RJ-45_TIA-568B_Right.png. [Accedido: 11-Abril-2022]
- [18] *Cableado genérico de telecomunicaciones para instalaciones de clientes*, TIA-568.0, Revisión C, Febrero, 2009 [En línea]. Disponible en: <https://global.ihs.com/>. [Accedido: 11-Abril-2022]
- [19] "Descripción general de la familia de normas ANSI/TIA 568-C." *Standards Informant*, 2022 [En línea]. Disponible en: <https://blog.siemon.com/standards/ansitia-568-c-family-of-standards-overview>. [Accedido: 11-Abril-2022]
- [20] *Cableado genérico de telecomunicaciones para instalaciones de clientes*, TIA-568.0, Revisión D, Septiembre, 2015 [En línea]. Disponible en: <https://global.ihs.com/>. [Accedido: 11-Abril-2022]
- [21] "ANSI/TIA 568.0-D Cableado genérico de telecomunicaciones para instalaciones de clientes", *Standards Informant*, 2022 [En línea]. Disponible en: <https://blog.siemon.com/standards/ansitia-568-c-0-generic-telecommunications-cabling-for-customer-premises>. [Accedido: 11-Abril-2022]
- [22] "ANSI/TIA 568.0-E Cableado genérico de telecomunicaciones para instalaciones de clientes", *Standards Informant*, 2022 [En línea]. Disponible en:

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

<https://blog.simon.com/standards/ansi-tia-568-0-e-generic-telecommunications-cabling-for-customer-premises>. [Accedido: 11-Abril-2022]

[23] "Subsistemas de cableado estructurado," *Wikimedia*, 2020 [En línea]. Disponible en: https://commons.wikimedia.org/wiki/File:Estructured_cabling_subsystems.svg.

[Accedido: 11-Abril-2022]

[24] G. G. Enrich, "El estándar TIA 942 - Una Visión General," *Ventas de Seguridad*, Vol. 11 Nº 4, 2007 [En línea]. Disponible en:

<http://www.areadata.com.ar/pdf/El%20standard%20TIA%20942%20-vds-11-4.pdf>.

[Accedido: 11-Abril-2022]

[25] "¿Qué es la seguridad de la información y cuantos tipos hay?", *ISOTools Excellence*, 2021 [En línea]. Disponible en: <https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/>. [Accedido: 11-Abril-2022]

[26] "Serie 27000", *ISO27000.ES*, 2005 [En línea]. Disponible en: <https://www.iso27000.es/iso27000.html>. [Accedido: 11-Abril-2022]

[27] "COBIT un marco de referencia ISACA", *ISACA*, 2022 [En línea]. Disponible en: <https://www.isaca.org/resources/cobit>. [Accedido: 11-Abril-2022]

[28] "Portal ISO 27000 en español", *ISO27000.ES*, 2005 [En línea]. Disponible en: <https://www.iso27000.es/iso27002.html>. [Accedido: 11-Abril-2022]

[29] ISACA, "COBIT5: Procesos Catalizadores", *StudyLib*, 2012 [En línea]. Disponible en: <https://studylib.es/doc/8972417/cobit-5---procesos-catalizadores>. [Accedido: 11-Abril-2022]

[30] Sindicatura General de la Nación. (Mayo, 2005) Resolución Nº48/05, Normas Control Interno Tecnología Información [En línea]. Disponible en:

<https://www.argentina.gob.ar/normativa/nacional/resolución-48-2005-106452>.

[Accedido: 11-Abril-2022]

[31] *Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para los controles de la seguridad de la información*, IRAM-ISO/IEC 27002 (Abril, 2021) [En línea]. Disponible en: <https://catalogo.iram.org.ar/#/normas/detalles/10611>.

[Accedido: 11-Abril-2022]

[32] Jefatura de Gabinete de Ministros. (Mayo, 2019) Resolución Nº 829/19, Estrategia Nacional de Ciberseguridad [En línea]. Disponible en:

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000->

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

324999/323594/norma.htm. [Accedido: 11-Abril-2022]

- [33] Boletín Oficial de la República Argentina. (Junio, 2021) Disposición Administrativa N° 641/21, Requisitos mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional [En línea]. Disponible en:
<https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628>. [Accedido: 11-Abril-2022]
- [34] Chaco Poder Ejecutivo. (Agosto, 2017) Decreto N° 1677/17 [En línea]. Disponible en:
<http://decretos.chaco.gov.ar>. [Accedido: 11-Abril-2022]
- [35] Chaco Poder Ejecutivo. (Noviembre, 2017) Resolución N° 2515/17 [En línea]. Disponible en:
<https://drive.google.com/file/d/1Y5RcQ00na8iRhCbFNCbEBCTXBgwehVTo/view?usp=sharing>. [Accedido: 11-Abril-2022]
- [36] Chaco Poder Ejecutivo. (Noviembre, 2018) Decreto N° 2743/18, Modelo de Políticas de Seguridad de la Información de la Provincia del Chaco [En línea]. Disponible en:
<http://decretos.chaco.gov.ar>. [Accedido: 11-Abril-2022]
- [37] Chaco Poder Legislativo. (Noviembre, 2020) Ley N° 3203-A, Simplificación y Modernización de la Administración [En línea]. Disponible en:
<http://www2.legislaturachaco.gov.ar:8000/Documentos/Ley/VistaPublicaLey/524182>. [Accedido: 11-Abril-2022]
- [38] A. Mejía Viteri y I. A. Murillo Tipán, "Diseño de un Data Center según las especificaciones de la norma ANSI/TIA 942 para el ISP Ecuonline S.A.", Tesis de Grado, Escuela Politécnica Nacional, Ecuador, 2014. [En línea]. Disponible en:
<https://bibdigital.epn.edu.ec/handle/15000/8921>. [Accedido: 11-Abril-2022]
- [39] J. Alvarado Tolentino, "Diseño de una infraestructura de telecomunicaciones con estándares de data center y redes, para garantizar la seguridad de la información y la transmisión de datos de los servidores de la Municipalidad Distrital de Independencia", Tesis de Grado, Universidad Nacional Santiago Antúnez, Mayolo-Perú, 2015 [En línea]. Disponible en: <http://repositorio.unasam.edu.pe/handle/UNASAM/1164>. [Accedido: 11-Abril-2022]
- [40] L. I. Bastidas Zambrano, E. C. Parrales Ruíz y J. V. León Acurio, *Los Sistemas de Redes en la Gestión Operativa*. Editorial CIDEPRO, 2019 [En línea]. Disponible en:
<http://sedici.unlp.edu.ar/handle/10915/81101>. [Accedido: 11-Abril-2022]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- [41] A. Y. Castro Tigua, "Estudio de normas técnicas para la distribución del espacio físico de las instalaciones del laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes", Tesis de Grado, Universidad Estatal del Sur, Manabí-Ecuador, 2021 [En línea]. Disponible en:
<http://repositorio.unesum.edu.ec/handle/53000/2817>. [Accedido: 11-Abril-2022]
- [42] Graciela E. Barchini, Mabel Sosa y Susana Herrera, "La informática como disciplina científica. Ensayo de mapeo disciplinar," *Rev. Informática Educ. y Medios Audiovisuales*, 2004 [En línea]. Disponible en:
<http://laboratorios.fi.uba.ar/lie/Revista/Articulos/010102/A1may2004.pdf>. [Accedido: 11-Abril-2022]
- [43] Chaco Poder Ejecutivo. (Octubre, 2020) Decreto N° 1283/20, Consejo de Transformación Digital [En línea]. Disponible en: <http://decretos.chaco.gov.ar>. [Accedido: 11-Abril-2022]
- [44] FOCO, "Agenda digital: se conformó un Consejo para promover la modernización del Estado", *Agencia chaqueña de noticias*, 2020 [En línea]. Disponible en: https://www.agenciafoco.com.ar/detalle_noticia/agenda-digital-se-conformo-un-consejo-para-promover-la-modernizacion-del-estado. [Accedido: 11-Abril-2022]
- [45] R. Hernández Sampieri, C. Fernández Collado y M. del P. Baptista Lucio, *Metodología de la Investigación*, 6ª Edición. 2017 [En línea]. Disponible en: <https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf>. [Accedido: 11-Abril-2022]
- [46] R. Hernández Sampieri, C. Fernández Collado y M. del P. Baptista Lucio, "Diseños del proceso de investigación cualitativa," en *Metodología de la Investigación*, 2017, pp. 468–506.
- [47] Instituto Nacional de Tecnología Industrial, "INTI", 2022 [En línea]. Disponible en: <https://www.argentina.gob.ar/inti>. [Accedido: 11-Abril-2022]
- [48] Asociación Electrotécnica Argentina, "AEA", 2022 [En línea]. Disponible en: <https://aea.org.ar/>. [Accedido: 11-Abril-2022]
- [49] C. V. Buitron Camúes, "Diseño de una red de datos y propuesta de plan de contingencia para el cableado estructurado del edificio de la Defensoría Pública del Ecuador de la ciudad de Quito." Tesis de Grado. Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Quito, Ecuador, 2017 [En línea]. Disponible en:

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

<https://bibdigital.epn.edu.ec/bitstream/15000/18816/1/CD-8203.pdf>. [Accedido: 11-Abril-2022]

- [50] D. I. J. Joscowicz, "Cableado Estructurado," *Material del Curso Comunicaciones Corporativas Unificadas*. Instituto de Ingeniería Eléctrica, Facultad de Ingeniería, Montevideo, Uruguay, 2013 [En línea]. Disponible en: <https://iie.fing.edu.uy/ense/assign/ccu/material/docs/Cableado%20Estructurado.pdf>. [Accedido: 11-Abril-2022]
- [51] Chaco Poder Ejecutivo. (Marzo, 2022) Decreto N° 483/22, Fideicomiso de Modernización del Estado [En línea]. Disponible en: <http://decretos.chaco.gov.ar>. [Accedido: 14-Abril-2022]
- [52] X-ROAD, "Software de capa de intercambio de datos de código abierto y gratuito," *X-Road® es una marca registrada de la Autoridad del Sistema de Información de Estonia (RIA)*, 2022 [En línea]. Disponible en: <https://x-road.global/>. [Accedido: 14-Abril-2022]
- [53] PNUD, "Sistema de Gestión para la Gobernabilidad (Sigob)", *Programa de Naciones Unidas para el Desarrollo*, 2022 [En línea]. Disponible en: <https://www.sigob.org/>. [Accedido: 14-Abril-2022]
- [54] Chaco día por día, "Capitanich relanzó el 'Sigob', para mejorar la eficacia de las políticas públicas", *La noticia entoda su dimensión*, 2020 [En línea]. Disponible en: <https://www.chacodiapordia.com/2020/03/07/capitanich-relanzo-el-sigob-para-mejorar-la-eficacia-de-las-politicas-publicas/>. [Accedido: 11-Abril-2022]
- [55] *Sistema de metas de la Gobernación del Chaco*. Resistencia: PNUD-SIGOB, 2020. [En línea]. Disponible en: <https://www.sigob.org/AR/Chaco/Metas/seguridad/login.aspx>
- [56] Chaco Poder Ejecutivo. (Agosto. 2020) Decreto N° 976/20, Estructura Orgánica Secretaría General de Gobernación [En línea]. Disponible en: <http://decretos.chaco.gov.ar>. [Accedido: 14-Abril-2022]

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Anexos

Anexo I: Formulario de relevamiento de infraestructura tecnológica



Dirección General de
Tecnologías de Información y Comunicación
Chaco Gobierno de todos



CHACO
Gobierno de todos

Formulario de Relevamiento de Infraestructura Tecnológica de Organismos

Sección 1: Datos Generales

Fecha: ____/____/____ (*)

Organismo (*)

Datos del Responsable Informático

DNI (*)

Apellido y Nombre (*)

Teléfono (*)

E-mail (*)

Oficina (*)

Observaciones



Sección 2: Servidores

¿Posee servidores? (*)	<input type="radio"/> SI Virtual: [.....] Físico: [.....] <input type="radio"/> NO
¿Quién los administra?	<input type="checkbox"/> ECOM Chaco S.A. <input type="checkbox"/> Personal Interno <input type="checkbox"/> Personal Externo <input type="checkbox"/> Sin administración
¿Todos los servidores cuentan con protección energética (UPS)?	<input type="radio"/> SI <input type="radio"/> NO
Cantidad de Servidores	<input type="checkbox"/> Tower: [.....] <input type="checkbox"/> Rackeables: [.....]
Indicar cuántos servidores X86 posee	<input type="checkbox"/> [.....]
Indicar cantidad de acuerdo a la marca	<input type="checkbox"/> Clones / PC Genérica: [.....] <input type="checkbox"/> IBM: [.....] <input type="checkbox"/> HP: [.....] <input type="checkbox"/> Dell: [.....] <input type="checkbox"/> Cisco: [.....] <input type="checkbox"/> Otros: [.....]
Indicar la cantidad según Sistema Operativo instalado	<input type="checkbox"/> Windows XP: [.....] <input type="checkbox"/> Windows 2000: [.....] <input type="checkbox"/> Windows 98: [.....] <input type="checkbox"/> Windows 2003: [.....] <input type="checkbox"/> Windows 2008: [.....] <input type="checkbox"/> Windows 2012: [.....] <input type="checkbox"/> Linux: [.....] <input type="checkbox"/> Unix: [.....] <input type="checkbox"/> Otro: [.....]
¿Los servidores cuentan con respaldo de datos?	<input type="radio"/> SI <input type="radio"/> NO
En caso de contar con respaldo, especificar el medio	<input type="checkbox"/> Óptico (CD – DVD) <input type="checkbox"/> Cinta <input type="checkbox"/> Discos rígidos <input type="checkbox"/> Otros
Indicar como se ejecuta el respaldo y archivado	<input type="radio"/> Automáticamente <input type="radio"/> Manualmente
¿Cuenta con archivado fuera de sitio?	<input type="radio"/> SI <input type="radio"/> NO
Observaciones	



Sección 3: Cuartos de Equipos/Comunicaciones

¿Cuenta con una habitación exclusiva para servidores y/o equipos de comunicaciones? (*)	<input type="radio"/> SI <input type="radio"/> NO
¿La habitación se encuentra refrigerada?	<input type="radio"/> SI <input type="radio"/> NO
¿Cuenta con línea eléctrica independiente?	<input type="radio"/> SI <input type="radio"/> NO
¿La habitación cuenta con algún mecanismo de seguridad de acceso?	<input type="checkbox"/> Llave <input type="checkbox"/> Huella dactilar <input type="checkbox"/> Iris <input type="checkbox"/> Tarjeta RFID <input type="checkbox"/> Otra <input type="checkbox"/> Ninguna
¿La habitación cuenta con sensores?	<input type="checkbox"/> Fuego <input type="checkbox"/> Humo <input type="checkbox"/> Temperatura <input type="checkbox"/> Humedad <input type="checkbox"/> Otro <input type="checkbox"/> Ninguno
Observaciones	

Sección 4: Red Interna

¿Quién la administra? (*)	<input type="checkbox"/> ECOM Chaco S.A. <input type="checkbox"/> Personal Interno <input type="checkbox"/> Personal Externo <input type="checkbox"/> Sin administración
¿Cuenta con Firewall? (*)	<input type="radio"/> SI <input type="radio"/> NO
Si cuenta con Firewall ¿de qué marcas?	<input type="checkbox"/> Fortinet <input type="checkbox"/> MS ISA Server/Forefront <input type="checkbox"/> Mikrotik <input type="checkbox"/> PFSense <input type="checkbox"/> BrazilFW <input type="checkbox"/> Linux con reglas personalizadas <input type="checkbox"/> Otro
El acceso a internet ¿por quién es provisto? (*)	<input type="checkbox"/> ECOM Chaco S.A. <input type="checkbox"/> Arnet/Telecom/Gigared/Fibertel <input type="checkbox"/> Modem 3g <input type="checkbox"/> Otros <input type="checkbox"/> No tiene
¿Posee Switches? (*)	<input type="radio"/> SI <input type="radio"/> NO
De los Switches especificar cantidad	<input type="checkbox"/> Administrables: [.....] <input type="checkbox"/> Estándares: [.....]
¿Todos los Switches se encuentran instalados en Racks? (*)	<input type="radio"/> SI <input type="radio"/> NO
¿El rack principal o central cuenta con línea eléctrica independiente? (*)	<input type="radio"/> SI <input type="radio"/> NO
¿El cableado de red se distribuye a través de bandejas? (*)	<input type="radio"/> SI <input type="radio"/> NO
Estado general del cableado del organismo (*)	<input type="radio"/> Bueno <input type="radio"/> Regular <input type="radio"/> Malo
Los dispositivos de conectividad cuentan con protección energética (UPS). (*)	<input type="radio"/> SI <input type="radio"/> NO
Cuenta con un diagrama actualizado de la red (*)	<input type="radio"/> SI <input type="radio"/> NO
Observaciones	

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Anexo II: Instructivo para formulario relevamiento de infraestructura tecnológica



Dirección General de
Tecnologías de Información y Comunicación
Chaco Gobierno de todos



Instructivo Formulario de Relevamiento de Infraestructura Tecnológica de Organismos

Contenido

1. Glosario	2
2. Estructura del Formulario de Relevamiento	2
3. Entrevistas	2
4. Instructivo para completar formulario	3
4.1 Sección 1: Datos Generales	3
4.2 Sección 2: Servidores	4
4.3 Sección 3: Cuartos de Equipos/Comunicaciones	6
4.4 Sección 4: Red Interna	7

1. Glosario

- **Administración de servidor:** nos referimos a la realización de tareas rutinarias sobre el *servidor físico o virtual*: de instalación, configuración, desinstalación de programas, reinicio del servidor o de servicios; o/y resolución de problemas de cualquier índole.
- **Responsable Informático (RI):** Es el personal técnico designado para responder las preguntas específicas relacionadas a la infraestructura tecnológica del organismo.

2. Estructura del Formulario de Relevamiento

El formulario es el instrumento mediante el cual se registra la información del relevamiento.

Consiste en ítems organizados en 4 secciones, las cuales se detallan a continuación:

- **Sección 1: Datos Generales** (se detalla la denominación del organismo y los datos generales del Responsable Informático designado para responder las preguntas acerca de la Infraestructura Tecnológica del organismo).
- **Sección 2: Servidores** (se detalla información sobre los servidores del organismo).
- **Sección 3: Cuartos de Equipos/Comunicaciones** (se detalla información sobre los cuartos de equipos y/o comunicaciones del organismo).
- **Sección 4: Red Interna** (se detalla información sobre la red interna del organismo).

3. Entrevistas

El relevamiento podrá requerir una o varias entrevistas.

En primera instancia, se solicita la designación de un Responsable Informático al organismo, y luego se registra los datos correspondientes del mismo en la sección 1.

En segunda instancia, se realizan las entrevistas a los Responsables Informáticos designados para brindar información acerca de la infraestructura tecnológica, y se registra la información en la sección 2, sección 3 y sección 4.



4. Instructivo para completar formulario

Se detalla a continuación las instrucciones específicas para completar cada sección del formulario.

4.1 Sección 1: Datos Generales

Fecha: ____/____/____ (*) Se anota la fecha en que se realiza la entrevista (Campo obligatorio)	
Organismo (*)	Denominación del organismo (Campo obligatorio)

Datos del Responsable Informático	
DNI (*)	Se registra el número de documento (Campo obligatorio)
Apellido y Nombre (*)	Se registra el nombre y apellido del RI (Campo obligatorio)
Teléfono (*)	Se consigan el /los número de celular/teléfono con su respectivo código de área, y si tuviera él/ los números de interno (Campo obligatorio)
Email (*)	Se registra la dirección electrónica del RI (Campo obligatorio)
Oficina (*)	Se registra la oficina del RI (Campo obligatorio)
Observaciones	Se detalla cualquier observación acerca del responsable informático. (Campo no obligatorio)



4.2 Sección 2: Servidores

<p>¿Posee servidores? (*)</p>	<p>Elegir la opción SI en caso que el organismo posea <i>servidores</i>, se indica la cantidad de Virtuales y Físicos. Si no posee servidor selecciona la opción NO y continúa con la Sección 3: Cuartos de Equipos/Comunicaciones. (Campo obligatorio)</p> <p><input type="radio"/> SI Virtual:[Numérico] Físico:[Numérico] <input type="radio"/> NO</p>
<p>¿Quién los administra?</p>	<p>Si en ítem ¿Posee Servidores? marcó la opción NO, esta opción no debe completarse. Puede seleccionar varias opciones. (Campo no obligatorio)</p> <p><input type="checkbox"/> ECOM Chaco S.A. <input type="checkbox"/> Personal Interno <input type="checkbox"/> Personal Externo <input type="checkbox"/> Sin administración</p>
<p>¿Todos los servidores cuentan con protección energética (UPS)?</p>	<p>Si en ítem ¿Posee Servidores? marcó la opción NO, esta opción no debe completarse. Elegir la opción SI en el caso que todos los servidores cuenten con protección, caso contrario marcar la opción NO. (Campo no obligatorio)</p> <p><input type="radio"/> SI <input type="radio"/> NO</p>
<p>Cantidad de Servidores</p>	<p>Indicar la cantidad de <i>servidores físicos</i> según sean TOWER o RACKEABLES. Si en ítem ¿Posee Servidores? marcó la opción NO, esta opción no debe completarse. (Campo no obligatorio)</p> <p><input type="checkbox"/> Tower: [Numérico] <input type="checkbox"/> Rackeables: [Numérico]</p>
<p>Indicar cuántos servidores X86 posee</p>	<p>Indicar cuantos son servidores X86, si posee. Por ej. si en el ítem anterior se indica: Tower: 2, Rackeables: 1, o sea son 3 servidores. En este ítem la cantidad ingresada no puede ser mayor a 3. Si en ítem ¿Posee Servidores? marcó la opción NO, esta opción no debe completarse. (Campo no obligatorio)</p> <p><input type="checkbox"/> [Numérico]</p>
<p>Indicar cantidad de acuerdo a la marca</p>	<p>Indicar las cantidades de <i>servidores físicos</i> para cada opción, según corresponda. Por ej. si en el ítem anterior se indica: Tower: 2, Rackeables: 1, o sea son 3 servidores, en este ítem la cantidad ingresada no puede ser mayor a 3. Si</p>

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"



	<p>en ítem ¿Posee Servidores? marcó la opción NO, esta opción no debe completarse. Puede seleccionar varias opciones. (Campo no obligatorio)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Clones / PC Genérica: [Numérico] <input type="checkbox"/> IBM: [Numérico] <input type="checkbox"/> HP: [Numérico] <input type="checkbox"/> Dell: [Numérico] <input type="checkbox"/> Cisco: [Numérico] <input type="checkbox"/> Otros: [Numérico]
<p>Indicar la cantidad según Sistema Operativo instalado</p>	<p>Indicar las cantidades de servidores para cada opción, según corresponda. Por ej. si en el ítem ¿Posee Servidores? se indica: Físico: 1 Virtuales 2., o sea son 3 servidores, en este ítem la cantidad ingresada no puede ser mayor a 3. Si en ítem ¿Posee Servidores? marcó la opción NO, esta opción no debe completarse. Puede seleccionar varias opciones. (Campo no obligatorio)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Windows XP: [Numérico] <input type="checkbox"/> Windows 2000: [Numérico] <input type="checkbox"/> Windows 98: [Numérico] <input type="checkbox"/> Windows 2003: [Numérico] <input type="checkbox"/> Windows 2008: [Numérico] <input type="checkbox"/> Windows 2012: [Numérico] <input type="checkbox"/> Linux: [Numérico] <input type="checkbox"/> Unix: [Numérico] <input type="checkbox"/> Otro: [Numérico]
<p>¿Los servidores cuentan con respaldo de datos?</p>	<p>Si elige la opción SI continúa con el siguiente ítem, en caso contrario si selecciona la opción NO continúa con el ítem Cuenta con archivado fuera de sitio. (Campo no obligatorio)</p> <ul style="list-style-type: none"> <input type="radio"/> SI <input type="radio"/> NO
<p>En caso de contar con respaldo, especificar el medio</p>	<p>Si en el ítem anterior marcó la opción SI, debe seleccionar el medio de respaldo, en caso de marcar la opción NO continúa con el ítem Cuenta con archivado fuera de sitio. Puede seleccionar varias opciones. (Campo no obligatorio)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Óptico (CD – DVD) <input type="checkbox"/> Cinta <input type="checkbox"/> Discos rígidos <input type="checkbox"/> Otros
<p>Indicar como se ejecuta el respaldo y archivado</p>	<p>Si en el ítem ¿Los servidores cuentan con respaldo de datos? marcó la opción SI, debe seleccionar el medio de respaldo, y como se ejecuta. En caso de marcar la opción</p>



	<p>NO continúa con el siguiente ítem. (Campo no obligatorio)</p> <p><input type="radio"/> Automáticamente</p> <p><input type="radio"/> Manualmente</p>
¿Cuenta con archivado fuera de sitio?	<p>Elegir la opción SI en el caso de que por lo menos un servidor cuente con archivado fuera de sitio, caso contrario marcar la opción NO. (Campo no obligatorio)</p> <p><input type="radio"/> SI</p> <p><input type="radio"/> NO</p>
Observaciones	<p>Se detalla cualquier observación acerca de los servidores físicos o virtuales. (Campo no obligatorio)</p>

4.3 Sección 3: Cuartos de Equipos/Comunicaciones

¿Cuenta con una habitación exclusiva para servidores y/o equipos de comunicaciones? (*)	<p>Si elige la opción SI continúa con el siguiente ítem, en caso contrario si selecciona la opción NO continúa con el ítem Sección 4: Red Interna. (Campo obligatorio)</p> <p><input type="radio"/> SI</p> <p><input type="radio"/> NO</p>
¿La habitación se encuentra refrigerada?	<p>Si en ítem ¿Cuenta con una habitación exclusiva para servidores y/o equipos de comunicaciones? marcó la opción NO, esta opción no debe completarse. (Campo no obligatorio)</p> <p><input type="radio"/> SI</p> <p><input type="radio"/> NO</p>
¿Cuenta con línea eléctrica independiente?	<p>Si en ítem ¿Cuenta con una habitación exclusiva para servidores y/o equipos de comunicaciones? marcó la opción NO, esta opción no debe completarse. (Campo no obligatorio)</p> <p><input type="radio"/> SI</p> <p><input type="radio"/> NO</p>
¿La habitación cuenta con algún	<p>Si en ítem ¿Cuenta con una habitación exclusiva para servidores y/o equipos de comunicaciones? marcó la</p>



mecanismo de seguridad de acceso?	opción NO , esta opción no debe completarse. Puede seleccionar varias opciones. (Campo no obligatorio) <ul style="list-style-type: none"> <input type="checkbox"/> Llave <input type="checkbox"/> Huella dactilar <input type="checkbox"/> Iris <input type="checkbox"/> Tarjeta RFID <input type="checkbox"/> Otra <input type="checkbox"/> Ninguna
¿La habitación cuenta con sensores?	Si en ítem ¿Cuenta con una habitación exclusiva para servidores y/o equipos de comunicaciones? marcó la opción NO , esta opción no debe completarse. Puede seleccionar varias opciones. (Campo no obligatorio) <ul style="list-style-type: none"> <input type="checkbox"/> Fuego <input type="checkbox"/> Humo <input type="checkbox"/> Temperatura <input type="checkbox"/> Humedad <input type="checkbox"/> Otro <input type="checkbox"/> Ninguno
Observaciones	Se detalla cualquier observación acerca de los cuartos de equipos y/o cuartos de comunicaciones. (Campo no obligatorio)

4.4 Sección 4: Red Interna

¿Quién la administra? (*)	Puede seleccionar varias opciones. (Campo obligatorio) <ul style="list-style-type: none"> <input type="checkbox"/> ECOM Chaco S.A. <input type="checkbox"/> Personal Interno <input type="checkbox"/> Personal Externo <input type="checkbox"/> Sin administración
¿Cuenta con Firewall? (*)	Si elige la opción SI continúa con el siguiente ítem, en caso contrario si selecciona la opción NO continúa con el ítem El acceso a internet ¿por quién es provisto? . (Campo obligatorio) <ul style="list-style-type: none"> <input type="radio"/> SI <input type="radio"/> NO
Si cuenta con Firewall ¿de qué marca es?	Si en ítem ¿Cuenta con Firewall? marcó la opción NO , esta opción no debe completarse. Puede seleccionar varias opciones. (Campo no obligatorio)

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"



	<input type="checkbox"/> Fortinet <input type="checkbox"/> MS ISA Server/Forefront <input type="checkbox"/> Mikrotik <input type="checkbox"/> PFSense <input type="checkbox"/> BrazilFW <input type="checkbox"/> Linux con reglas personalizadas <input type="checkbox"/> Otro
El acceso a internet ¿por quién es provisto? (*)	Puede seleccionar varias opciones. (Campo obligatorio) <input type="checkbox"/> ECOM Chaco S.A. <input type="checkbox"/> Arnet/Telecom/Gigared/Fibertel <input type="checkbox"/> Modem 3g <input type="checkbox"/> Otros <input type="checkbox"/> No tiene
¿Posee Switches? (*)	Si elije la opción SI continúa con el siguiente ítem, en caso contrario si selecciona la opción NO continúa con el ítem ¿El rack principal o central cuenta con línea eléctrica independiente? . (Campo obligatorio) <input type="radio"/> SI <input type="radio"/> NO
De los Switches especificar cantidad	Si en ítem ¿Posee Switches? marcó la opción NO , esta opción no debe completarse. (Campo no obligatorio) <input type="checkbox"/> Administrables: [Numérico] <input type="checkbox"/> Estándares: [Numérico]
¿Todos los Switches se encuentran instalados en Racks? (*)	Elegir la opción SI en el caso que todos los switches estén en rack, caso contrario marcar la opción NO . (Campo obligatorio) <input type="radio"/> SI <input type="radio"/> NO
¿El rack principal o central cuenta con línea eléctrica independiente? (*)	Elegir la opción SI en el caso que el rack principal cuente con una línea eléctrica independiente, caso contrario marcar la opción NO . (Campo obligatorio) <input type="radio"/> SI <input type="radio"/> NO
¿El cableado de red se distribuye a través de bandejas? (*)	Elegir la opción SI en el caso que todos los cables se distribuyan en bandejas, caso contrario marcar la opción NO . (Campo obligatorio) <input type="radio"/> SI <input type="radio"/> NO
Estado general del cableado del organismo (*)	Completar de acuerdo a los siguientes criterios: <ul style="list-style-type: none"> • Con Bueno si el tendido de cables de red se encuentra con cable canal y con rosetas, o empotrado dentro de las paredes.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"



	<ul style="list-style-type: none"> • Con Regular si el tendido de cables no se encuentra con cable canal, con rosetas dañadas, o sin éstas. • Con Malo en caso que los cables se encuentren dañados, dispuestos por el piso en las oficinas y expuestos al deterioro por el paso de personas. <p>(Campo obligatorio)</p> <p><input type="radio"/> Bueno</p> <p><input type="radio"/> Regular</p> <p><input type="radio"/> Malo</p>
Los dispositivos de conectividad cuentan con protección energética (UPS). (*)	<p>Elegir la opción SI en el caso que todos los dispositivos cuenten con protección eléctrica, caso contrario marcar la opción NO. (Campo obligatorio)</p> <p><input type="radio"/> SI</p> <p><input type="radio"/> NO</p>
Cuenta con un diagrama actualizado de la red (*)	<p>Elegir la opción SI en el caso que todo el organismo cuente con un diagrama de red actualizado, caso contrario marcar la opción NO. (Campo obligatorio)</p> <p><input type="radio"/> SI</p> <p><input type="radio"/> NO</p>
Observaciones	<p>Se detalla cualquier observación acerca de la red interna, como por ejemplo de los dispositivos de conectividad, etc. (Campo no obligatorio)</p>

Anexo III: Informe de Infraestructura Tecnológica 5º Piso Casa de Gobierno



INFORME DE INFRAESTRUCTURA TECNOLÓGICA DEL 5º PISO DE CASA DE GOBIERNO

Actualmente la red de datos del 5º piso de Casa de Gobierno, posee una administración descentralizada, ya que tiene una topología mixta o híbrida, en la cual coexisten dos o más topologías de red diferentes. Estas subredes son administradas por técnicos de la empresa Ecom Chaco S.A. y por técnicos pertenecientes al organismo. Lo óptimo sería implementar una red con administración centralizada, que sea administrada por un sólo administrador de red o un equipo técnico que haga sus veces, con la existencia de un rack de comunicaciones principal, del cual se desprendan conexiones hacia las áreas de trabajo, o hacia otros rack de comunicaciones secundarios.

Es importante resaltar que los datos del relevamiento efectuado en el 5º Piso de Casa de Gobierno, han sido sometidos a una evaluación de riesgos de su infraestructura tecnológica.

Ítem	Riesgo	Estimación del riesgo	Salvaguardas implementadas
1	Servidores sin respaldo de datos	Apreciable	Backup automático en discos rígidos
2	Los servidores no cuentan con una protección energética (UPS)	Importante	Sin salvaguardas
3	Espacio físico no delimitado	Crítico	Sin salvaguardas
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco SA
Resultado de la estimación de riesgos		Negativo	

Por lo antes observado se concluye, que el resultado de la estimación de riesgos de la infraestructura tecnológica del organismo es negativo, debido a que de 6 ítems considerados en el análisis, sólo 2 tienen implementadas salvaguardas, mientras que los 4 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"



Dirección General de
Tecnologías de Información y Comunicación
Chaco Gobierno de todos



Por lo tanto para facilitar el trabajo diario de los empleados públicos del organismo, con el objetivo de mejorar la calidad en el servicio de conectividad y la infraestructura tecnológica del quinto piso, a fin de dar soporte a las tecnologías y sistemas utilizados que brindan servicios a los ciudadanos, resulta necesario trabajar sobre el **diseño del cableado horizontal del piso**.

El mismo requiere la **construcción de una sala tecnológica segura**, que contemple requerimientos de seguridad física y ambiental para el alojamiento de los equipos y recursos de conectividad, que permita centralizar y administrar los dispositivos, junto a la **normalización del cableado estructurado**.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

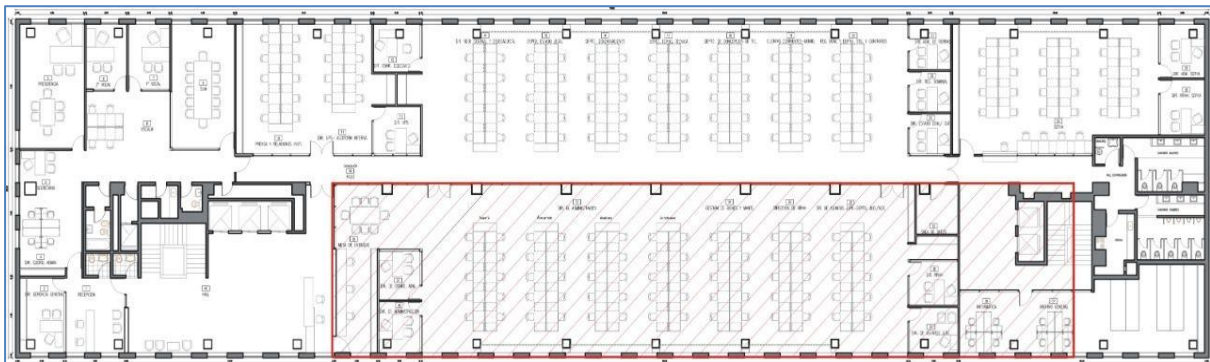
Estimación de costos asociados a la implementación de STS

A	B	C	D	E	F	G	
1	Total de Costos Sala Tecnológica Segura y Sistema de Cableado Estructurado para 117 puestos nuevos		\$32.706,00	Dólares			
2							
3	Equipamiento TIC Sala Segura		\$7.839,74				
4	Elementos de cableado estructurado Sala Segura		\$5.737,04				
5	Elementos de cableado estructurado despliegue horizontal		\$12.276,70				
6	Obra Civil Sala Segura		\$6.852,52				
7							
8	Categoría	Ítem y Descripción	Unidad	Costo	Cantidad	Total	Aclaraciones
9	Equipamiento TIC Sala Segura	alimentación. Modelo sugerido: Mikrotik Ccr1016-12s-1s+	U	\$1.638,44	1	\$1.638,44	Conectividad
10		Mikrotik CRS326-24G-2S+RM	U	\$501,04	5	\$2.505,18	
11		Modulo SFP+ Mikrotik para conexión sala central con sala segura de cada piso.	U	\$408,51	2	\$817,03	
12		Switch 16/24 puertos SFP+. Modelo sugerido: Mikrotik 317-1G-16S+RM	U	\$914,46	1	\$914,46	
13		Direct attach Mikrotik de 3 mts. Para conexión de backbone.	U	\$154,94	0	\$0,00	
14		Direct attach Mikrotik de 2 mts. Para conexión de backbone.	U	\$126,02	2	\$252,04	
15	Direct attach Mikrotik de 1 mts. Para conexión de backbone.	U	\$121,89	5	\$609,43		
16	UPS rackable administrable 1,5 KVA batería interna	U	\$1.103,17	1	\$1.103,17	Protección	
17						\$7.839,74	
18							
19	Elementos de cableado estructurado en Sala Tecnológica Segura	Rack de 19" 45 unidades (Rack Evo Iv 45u 1000mm Gabitel R-e4-45u)	U	\$1.820,09	1	\$1.820,09	Organización central del cableado horizontal
20		Canal de tensión 5/6 tomas	U	\$106,12	2	\$212,25	
21		Patch panel Cat. 6 24 bocas	U	\$388,09	5	\$1.940,44	
22		Organizador de cables 2u	U	\$34,52	5	\$172,60	
23		Patchcords cat. 6 de 0,50 cm.	U	\$9,21	70	\$645,00	
24		Patchcords cat. 6 de 1 m.	U	\$15,89	47	\$746,67	
25	Mano de Obra	Hs	\$10,00	20	\$200,00		
26						\$5.737,04	
27							
28	Elementos de cableado estructurado en distribución de la planta	Bandeja portacable de 100 mm.	U	\$20,77	7	\$145,36	
29		Bandeja portacable de 300 mm.	U	\$48,79	11	\$536,74	
30		Bandeja portacable de 400 mm.	U	\$65,82	5	\$329,08	
31		SopORTE tipo trapecio para bandeja portacable de 100 mm.	U	\$3,00	14	\$41,94	
32		SopORTE tipo trapecio para bandeja portacable de 300 mm.	U	\$4,06	22	\$89,37	
33		SopORTE tipo trapecio para bandeja portacable de 400 mm.	U	\$5,51	10	\$55,15	
34		Varilla Roscada de 8mm con sus respectivas tuercas y arandelas.	U	\$3,22	92	\$296,48	
35		taco metalico p/hormigon 8mm	U	\$2,11	92	\$194,12	
36		Reducción para bandeja portacable: de 300 a 200, mm.	U	\$17,68	2	\$35,36	
37		Empalme para bandeja portacable	U	\$1,43	18	\$25,74	
38		Curva plana de 90° para bandeja portacable de 400 mm.	U	\$14,41	2	\$28,82	
39		Derivación universal para bandeja portacable de 2 piezas, ancho variable.	U	\$2,61	1	\$2,61	
40		Curva vertical articulada para bandeja portacable de 400 mm.	U	\$12,48	1	\$12,48	
41		Unicanal 100x50 mm (se usa como referencia Hellermann Tyton)	U	\$34,52	22	\$759,43	
42	Face plate para 4 tomas rj-45 para unicanal (FpwcB)	U	\$8,40	31	\$260,31		
43	Caja de cable de 305 mts. Cat. 6 (referencia: Furukawa)	U	\$315,53	15	\$4.732,95		
44	Jack RJ-45 Cat. 6 (referencia: marca GLC)	U	\$9,59	117	\$1.122,03		
45	Patchcords cat. 6 de 1 m.	U	\$15,89	117	\$1.858,72		
46	Mano de Obra	Hs	\$10,00	175	\$1.750,00		
47						\$12.276,70	
48							
49							
50	Obra Civil Sala Segura	para equipos de AA y tableros. Lana de vidrio 50 mm	m2	\$31,50	42	\$1.323,00	Construcción en seco
51		Baldosas de goma 50x50 3,2 mm Tipo Deco de Indelval	m	\$49,00	12,25	\$600,25	Piso
52		Zócalo de MDF prepint. 70 mm de altura, 3,4" esp. Sin molduras	m	\$10,20	28	\$285,60	Zócalos
53		Pintura latex para interiores	m2	\$7,50	89,6	\$672,00	Pintura
54		Esmalte sintético sobre puerta metálica	m2	\$9,50	3,87	\$36,77	
55		Pintura de losa existente	m2	\$8,40	12,25	\$102,90	
56		Pintura Identificación STS Piso y unidad	GL	\$13,50	1	\$13,50	
57		Puerta de rebatir (910x2200) RF60 Rejilla vent. Barral antipánico; Burletes;	GL	\$386,00	1	\$386,00	Carpintería
58		Tablero Electrico de corte General, monofásico	GL	\$103,00	1	\$103,00	Instalación eléctrica
59		Artefactos de Ilum. Marea LED, instalado	ud	\$42,50	3	\$127,50	
60		Bocas de luz	ud	\$45,00	5	\$225,00	
61		Toma exterior	ud	\$42,00	4	\$168,00	
62		Toma A20	ud	\$42,00	1	\$42,00	
63		Artefacto luz de emergencia, instalado	ud	\$39,00	1	\$39,00	
64	Puesta a Tierra	ud	\$89,00	1	\$89,00		
65	Bandejas Datos y Energía	GL	\$519,00	1	\$519,00		
66	Alimentación desde TGP hasta tablero de sala, con protección	GL	\$206,00	1	\$206,00		
67	Provisión y Montaje un (1) Aire Split AA 4500 fg/h frio solo. Clase A. Gas Eco. R410a. Autoencend. Auto-diag. Falta gas refriger. Bloqueo del equipo cuando disminuye carga del liquido ref. Garantía 2 años.	ud	\$619,00	1	\$619,00	Sistema de Refrigeración	
68	VF30, denominación: Fingerprint Access Control.	ud	\$210,00	1	\$210,00	Control de Acceso	
69	Carteles de Salida, Señalética seguridad, instalado	GL	\$39,00	1	\$39,00		
70	Sensor de Temperatura, instalado	U	\$107,00	1	\$107,00	INSTALACIONES CONTRA INCENDIO	
71	Sensor de humo, instalada	U	\$107,00	1	\$107,00		
72	Central de Incendio, 1 lazo, convencional, instalada	U	\$780,00	1	\$780,00		
73	Matafuego ABC 5 kg, IRAM, baliza. Carga vigente 1 año-	U	\$52,00	1	\$52,00		
74						\$6.852,52	

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

	A	B	C	D	E
1	Total de Costos SISTEMA DE VIDEOVIGILANCIA 17 cámaras			\$2.696,68	Dólares
2					
3					
4	Item	Descripción	Cantidad	Precio U.	Total U\$
5	NVR	Hikvision. Mod.:DS-7732NI-K4	1	\$730,00	\$730,00
6	disco rigido	2 Tb. W. Digital. Mod.:purpura	1	\$115,00	\$115,00
7	camara	Hikvision. Mod.:DS-2CE56D0T-IPF(turbo)	17	\$25,00	\$425,00
8	cable UTP	cat. 6 referencia furukawa	2	\$315,53	\$631,06
9	Patchs p/conexión	1 mts. cat. 6 referencia furukawa	18	\$15,89	\$286,02
10		0,50 mts. cat. 6 referencia furukawa	17	\$9,21	\$156,57
11	jack rj-45(8p8c)	cat. 6 referencia furukawa	17	\$9,59	\$163,03
12	mano obra	expresada en hs	19	\$10,00	\$190,00
13					\$2.696,68

Propuesta de remodelación 5º Piso, con 1 STS y 117 puestos



Link para descarga de la Estimación de costos del 5º Piso (Acceso Público)

<https://drive.google.com/drive/folders/1TxYUy9mSsGJChG1bOTz40vkDWAXvYdRG?usp=sharing>

Anexo IV: Políticas de Seguridad de la Información aplicables a las STS

INTRODUCCIÓN

La presente política tiene como objeto gestionar la seguridad de la información de las Salas Tecnológicas Seguras en el marco de un Sistema de Cableado Estructurado, atendiendo a:

- Gestión de Activos
- Control de Accesos
- Seguridad Física y Ambiental
- Seguridad en las Telecomunicaciones

MARCO INSTITUCIONAL

- Ley N° 3203-A de simplificación, racionalización y modernización administrativa, de la Administración Pública Provincial [37].
- Decreto N° 2743/2018 del Poder Ejecutivo del Chaco aprueba el "Modelo de Políticas de Seguridad de la Información de la Provincia del Chaco"[36].
- Decreto N° 976/2020, aprueba la estructura organizativa de la jurisdicción Secretaría General de Gobernación, y en página 102 establece la responsabilidad primaria y las acciones de la Dirección General de Tecnologías de Información y Comunicación [56].

TÉRMINOS Y DEFINICIONES

Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

1. Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
2. Integridad: se salvaguarda la exactitud y totalidad de la información, como así también, los métodos de procesamiento.
3. Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

A los efectos de una correcta interpretación de la presente política, se realizan las siguientes definiciones.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

1. Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
2. Activo: Algo que presenta valor para la organización.
3. Activo de información: Es todo aquello que comprende la información o los elementos que la contienen o permiten su procesamiento y, en consecuencia, debe ser protegido.
4. Activo de Soporte: Son los que se incluyen dentro de hardware, software, redes, personal, sitio, servicio, etc.
5. Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
6. Tecnología de la Información: Se refiere al hardware y software operados por el área o por un tercero que procese información en su nombre, para llevar a cabo una función propia del área, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
7. Propietario de la Información: Debe ser entendido desde su acepción técnica, no jurídica, donde se define que es un individuo o entidad, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona disponga de los derechos de propiedad reales del activo.
8. Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

ORGANIZACIÓN DE LA SEGURIDAD

Cada organismo deberá designar un Responsable Informático, el cual cumplirá funciones de Responsable de Seguridad de la Información. El mismo deberá supervisar el cumplimiento de la presente política aplicable a las STS.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

8. Cláusula: Gestión de Activos

Generalidades

El organismo debe tener un conocimiento preciso sobre los activos que posee en la Sala Tecnológica Segura, como parte importante de la administración de riesgos. Algunos ejemplos de activos que se pueden encontrar en la STS son:

- Activos físicos: equipamiento informático (servidor tower, servidor rackeable, monitor, etc.), equipos de comunicaciones (router, switch, etc.), medios magnéticos (cintas, discos, etc.), otros equipos técnicos (rack, ups, unidades de aire acondicionado, controles automatizados de acceso, etc.).
- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

Objetivo

- Garantizar que los activos de información de las Salas Tecnológicas Seguras reciban un apropiado nivel de protección.

Alcance

- Esta política se aplica a todos los activos de información que forman parte de la STS administrada por el organismo.

Responsabilidad

- El Responsable de Seguridad de la Información es el encargado de los activos físicos y recursos de información alojados en las STS. Para ello deberá aplicar los lineamientos de la presente política a la utilización de los recursos de la tecnología de información. Dichos lineamientos cumplen con los pilares de seguridad de la información: disponibilidad, confidencialidad e integridad según corresponda.

Política

8.1 Categoría: Responsabilidad sobre los activos

Objetivo

Todos los activos alojados en la STS deben ser inventariados y contar con un propietario nombrado. En el caso de los activos físicos deben contener el N° de Registro Patrimonial correspondiente.

8.1.1 Control: Inventario de activos

Se deben identificar los activos de información alojados en la STS del organismo. Existen muchos tipos de activos, que incluyen:

- a) información: bases de datos, archivos de datos, documentación, contratos, acuerdos;
- b) activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios;
- c) activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos;
- d) instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua, etc.;
- e) servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: iluminación, energía, y aire acondicionado;
- f) personas, y sus calificaciones, habilidades y experiencia.

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 12 meses.

El encargado debe elaborar el inventario y mantenerlo actualizado.

8.1.2 Control: Propiedad de los activos

Toda la información y los activos alojados en las STS, junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en el área.

Se designarán los propietarios de los activos identificados, quienes deben cumplir sus funciones de propietario, esto es:

- a) informar sobre cualquier cambio que afecte el inventario de activos;

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- b) clasificar los activos en función a su valor;
- c) definir los requisitos de seguridad de los activos;
- d) velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

8.2 Categoría: Clasificación de la información

Objetivo

Asegurar que la información alojada en las STS reciba un nivel de protección apropiado.

La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

8.2.1 Control: Directrices de clasificación

Para clasificar un activo de información alojado en una STS, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece la metodología de clasificación de la información propuesta en función a cada una de las mencionadas características:

Confidencialidad:

0. Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del organismo o no. PUBLICO
1. Información que puede ser conocida y utilizada por todos los empleados del organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el organismo, el sector público o terceros. RESERVADA - USO INTERNO
2. Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al organismo, al sector público o a terceros. RESERVADA - CONFIDENCIAL
3. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del organismo, y cuya divulgación o uso

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

no autorizados podría ocasionar pérdidas graves al mismo, al sector público o a terceros. RESERVADA SECRETA

Integridad:

0. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del organismo.
1. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el organismo, el sector público o terceros.
2. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el organismo, el sector público o terceros.
3. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al organismo, al sector público o a terceros.

Disponibilidad:

0. Información cuya inaccesibilidad no afecta la operatoria del organismo.
1. Información cuya inaccesibilidad permanente durante un plazo de tiempo podría ocasionar pérdidas significativas para el organismo, el sector público o terceros.
2. Información cuya inaccesibilidad permanente durante un plazo de tiempo mayor a un día podría ocasionar pérdidas significativas al organismo, al sector público o a terceros.
3. Información cuya inaccesibilidad permanente durante un plazo de tiempo no menor a una hora, podría ocasionar pérdidas significativas al organismo, al sector público o a terceros.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- CRITICIDAD BAJA: ninguno de los valores asignados supera el 1.
- CRITICIDAD MEDIA: alguno de los valores asignados es 2.
- CRITICIDAD ALTA: alguno de los valores asignados es 3.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Sólo el propietario de la información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al responsable de seguridad de la información.
- Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deben tener acceso a la misma.

9. Cláusula: Control de Accesos

Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información alojados en las STS, se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Objetivo

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información alojados en las STS. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red del organismo y otras redes públicas o privadas.

Alcance

- La política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información alojados en la STS del organismo, cualquiera sea la función que desempeñe.
- Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad

El Responsable de Seguridad de la Información estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario alojados en las STS; el monitoreo del uso de las instalaciones de procesamiento de la información.

Los propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información alojada en la STS, con el objeto de determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.

Política

9.1 Categoría: Requerimientos para la Gestión de Acceso

Objetivo

Controlar el acceso a la información contenida en la STS. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos sobre la base de los requerimientos del organismo y de seguridad. Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

9.1.1 Control: Política de Gestión de Accesos

En la aplicación de gestión de acceso, se contemplarán los siguientes aspectos:

- a) Identificar los requerimientos de seguridad de cada una de las aplicaciones alojadas en las STS.
- b) Identificar toda la información relacionada con las aplicaciones.
- c) Establecer criterios coherentes entre esta política de control de acceso y la política de clasificación de información de los diferentes sistemas y redes (Ver cláusula 8 Gestión de Activos).
- d) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.

9.1.2 Control: Reglas de Gestión de Acceso

Las reglas de control de acceso especificadas, deben:

- a) Indicar expresamente si las reglas son obligatorias u optativas.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- b) Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".

9.2 Categoría: Administración de Gestión de Usuarios

Objetivo

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información alojados en las STS.

9.2.1 Control: Registración de Usuarios

El Responsable de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información alojados en las STS, el cual debe:

- a) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- b) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- c) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- d) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del organismo o sufrieron la pérdida/robo de sus credenciales de acceso.

9.2.2 Control: Gestión de Privilegios

Se deberá limitar y controlar la asignación y uso de privilegios de los sistemas alojados en las STS, debido a que el uso inadecuado de ellos contribuye a la falla de los sistemas. Los sistemas que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- d) Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad de la Información.

9.3 Categoría: Responsabilidades del Usuario

Objetivo

Evitar el acceso de usuarios no-autorizados a las STS, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información. Para ello la cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deberán estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas.

9.3.1 Control: Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios autorizados deben cumplir las siguientes directivas:

- a) Mantener las contraseñas en secreto.
- b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema alojado en la STS.
- c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas que se trate.

11. Cláusula: Seguridad Física y Ambiental

Generalidades

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

La seguridad física y ambiental de las STS, brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del organismo. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del organismo, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y comunicación, minimizando las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones de la STS del organismo, como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del organismo.

Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente a la STS del organismo, pero situado físicamente fuera del mismo ("housing"), así como en equipamiento ajeno al organismo, pero que albergue sistemas y/o preste servicios de procesamiento de información al organismo ("hosting").

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencias a las instalaciones e información alojada en las STS del organismo.

Proteger el equipamiento de procesamiento de información crítica del organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático ubicado en la STS, que contiene información del organismo.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información alojados en las STS del organismo: instalaciones, equipamiento, etc.

Responsabilidad

El Responsable de Seguridad de la Información definirá junto con el los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en la presente Cláusula.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones de las STS del organismo, con información de su incumbencia cuando lo crean conveniente.

Política

11.1 Categoría: Áreas Seguras

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia a la información alojada en la STS del Organismo.

Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

11.1.1 Control: Perímetro de seguridad física

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas en las STS del organismo y de las instalaciones de procesamiento de información.

El organismo deberá utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, equipos de comunicación de datos, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información alojados en la STS. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

- a) Definir y documentar claramente el perímetro de seguridad de la STS.
- b) Ubicar las instalaciones de procesamiento de información y equipos de comunicación de datos dentro de un área de construcción físicamente sólida (por ejemplo, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- c) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.

11.1.2 Control: Controles físicos de entrada

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad de la Información, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

- a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- b) Controlar y limitar el acceso a la información clasificada, a las instalaciones de procesamiento de información, y equipos de comunicación de datos exclusivamente a las personas autorizadas. Se utilizarán controles de autenticación para autorizar y validar todos los accesos de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal (PIN), etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.
- c) Revisar y actualizar cada 6 meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable del Área de la que dependa.
- d) Revisar los registros de acceso a las áreas protegidas.

11.1.4 Control: Protección contra amenazas externas y de origen ambiental

Se debe asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se debe prestar consideración a cualquier amenaza contra la seguridad presentada por áreas vecinas; por ejemplo, un fuego en una oficina vecina, escape de agua en el techo o pisos.

Se debe considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

- a) Los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área protegida. Los suministros a granel como papelería no deben almacenarse en el área protegida.
- b) Se debe proporcionar equipo contra-incendios ubicado adecuadamente.

11.1.5 Control: Trabajo en áreas seguras

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

- a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.
- e) Prohibir comer, beber y fumar dentro de las áreas protegidas.

11.2 Categoría: Seguridad de los equipos

Objetivo

Evitar pérdida, daño, robo o compromiso de los activos alojados en las STS y la interrupción de las actividades del organismo.

Se debe proteger los equipos de amenazas físicas y ambientales.

11.2.1 Control: emplazamiento y protección de equipos

El equipamiento será ubicado en la STS y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

- a) Ubicar el equipamiento en la STS, donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en la STS y que permita la supervisión durante su uso.
- c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

Se deben establecer lineamientos sobre las actividades de comer, beber y fumar en la STS, y en proximidad de los medios de procesamiento de la información.

Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información.

11.2.2 Control: Instalaciones de suministro

El equipamiento alojado en la STS, estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- b) Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento alojado en la STS que sustenta las operaciones críticas del organismo. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Debe realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa.

Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

11.2.3 Control: Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra interceptación o daño, mediante las siguientes acciones:

- a) Cumplir con los requisitos técnicos vigentes de la República Argentina.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

- b) Utilizar cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a protección alternativa.
- c) Proteger el cableado de red contra interceptación no autorizada o daño.
- d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
- e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

Para los sistemas sensibles o críticos, se implementarán los siguientes controles adicionales:

- a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
- b) Utilizar rutas o medios de transmisión alternativos.

11.2.4 Control: Mantenimiento de los equipos

Se realizará el mantenimiento del equipamiento alojado en la STS para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables de Seguridad de la Información del organismo. El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- d) Registrar el retiro de equipamiento de la STS del organismo para su mantenimiento.
- e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

11.2.5 Control: Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la STS del organismo, será autorizado por el responsable patrimonial. En el caso de que en el

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

mismo se almacene información clasificada, debe ser aprobado además por el propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro de la STS del organismo para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento.

13. Cláusula: Seguridad en las Comunicaciones

Generalidades

Los sistemas de información están comunicados entre sí, tanto dentro del organismo como con terceros fuera de él. Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información alojada en la STS, que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Alcance

Todas las instalaciones de procesamiento y transmisión de información alojadas en la STS del organismo.

Responsabilidad

El Responsable de Seguridad de la información deberá verificar el cumplimiento de las normas, procedimientos y controles establecidos.

Política

13.1 Categoría: Gestión de la Red

Objetivo

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

13.1.1 Control: Controles de red

El Responsable de Seguridad de la Información definirá controles en la STS, para garantizar la seguridad de los datos y los servicios conectados en las redes del organismo, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- a) Establecer los procedimientos para la administración del equipamiento en forma remota, la que será llevada a cabo por el responsable establecido.
- b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
- c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

13.1.2 Control: Mecanismos de seguridad asociados a servicios en red.

El Responsable de Seguridad de la Información junto con el/los administrador/es de red, definirán las pautas para garantizar la seguridad de los servicios de red del organismo, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- a) Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- b) Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- c) Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- d) Instalar periódicamente las actualizaciones de seguridad.
- e) Dicha configuración será revisada periódicamente por el Responsable de Seguridad de la Información.

Link para descarga de las PSI (Acceso Público)

<https://drive.google.com/drive/folders/19ZRz-80SNr257km401uAxjXDZLbjn?usp=sharing>

Anexo V: Planos con especificaciones de STS

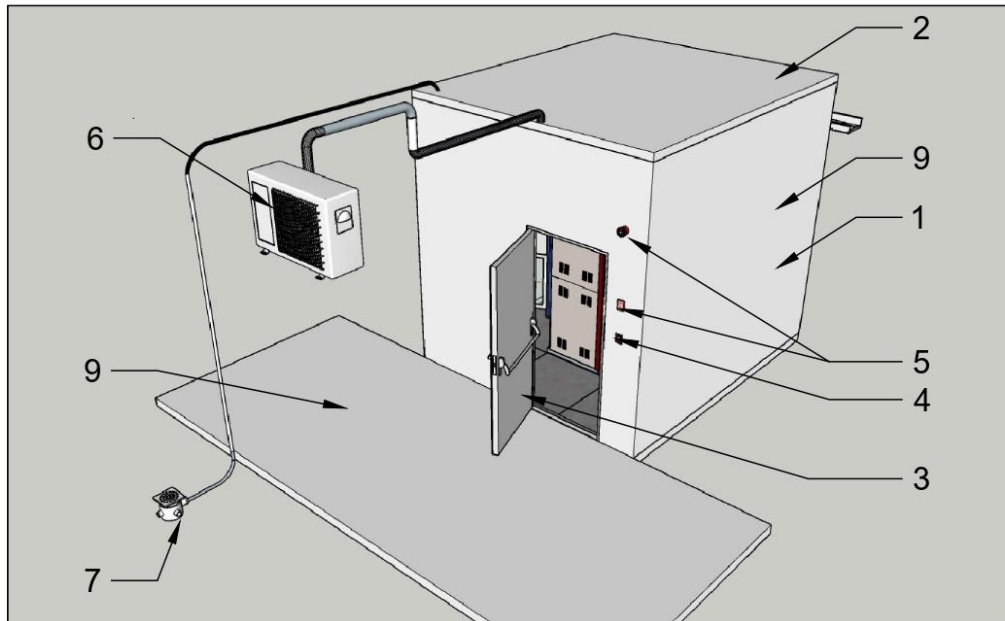


FIGURA 1 - VISTA DEL FRENTE

- 1- Recinto resistente al fuego de sesenta minutos. (RF60)
Diseño y materiales deben proporcionar protección antivandálica, de acuerdo a nivel de seguridad requerido por la situación. Pisos, Paredes, cielorrasos, deberán sellarse, ser pintados y construidos con materiales que logren minimizar el polvo. Terminaciones de color claro para mejorar la iluminación de la Sala.
- 2- Cielorraso Rf60. Altura mínima: 2.60 m.
En caso de existir losa de hormigón armado, las paredes RF60 llegarán hasta la losa, a la que sólo se la enprolija y pinta. Se evitará la construcción del cielorraso. El Espacio deberá ser liberado de todo tipo de instalaciones preexistentes. De existir, se deberá eliminar caños de agua o desagües en el área de la sala segura.
- 3- Puerta cortafuego Rf60 con homologación de INTI. Apertura hacia afuera. Doble contacto en sus cuatro lados, con burletes intumescentes. Dimensión mínima: 1.00 m por 2.05 m de alto. Cerradura reforzada del tipo doble tambor de bronce o biométrica como parte del sistema de control de acceso. Deberá garantizar una fácil apertura desde el exterior o interior, sin depender exclusivamente de mecanismo o sistemas electrónicos. Barral antipánico en el interior.
- 4- Sistema de control de acceso biométrico.
- 5- Pulsador y sirena de alarma contra incendio en el exterior de la SS.
- 6- Unidad exterior de AA sistema separado.
- 7- Desagüe de agua de condensación impulsada con bomba tipo Mini Orange Aspen Pumps según cálculo de altura y caudal, hasta desagües de la Inst. Sanitaria.
- 9- Pasillo semipúblico que permita el acceso directo del personal autorizado sin pasar por otros lugares restringido para acceder a la Sala Segura a cualquier hora.

PROVINCIA DEL CHACO	SUBSECRETARIA DE PLANIFICACIÓN Y PROYECTOS		PLANO N°:
MPEI	DIRECCION DE PROYECTOS		F1
OBRA: SALA SEGURA		ESCALA: S/E	
UBICACION: -----		FECHA	
PLANO: IMAGENES SALA SEGURA – VISTA DEL FRENTE		08/21	
EQUIPO DE TRABAJO: RF/MS			

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

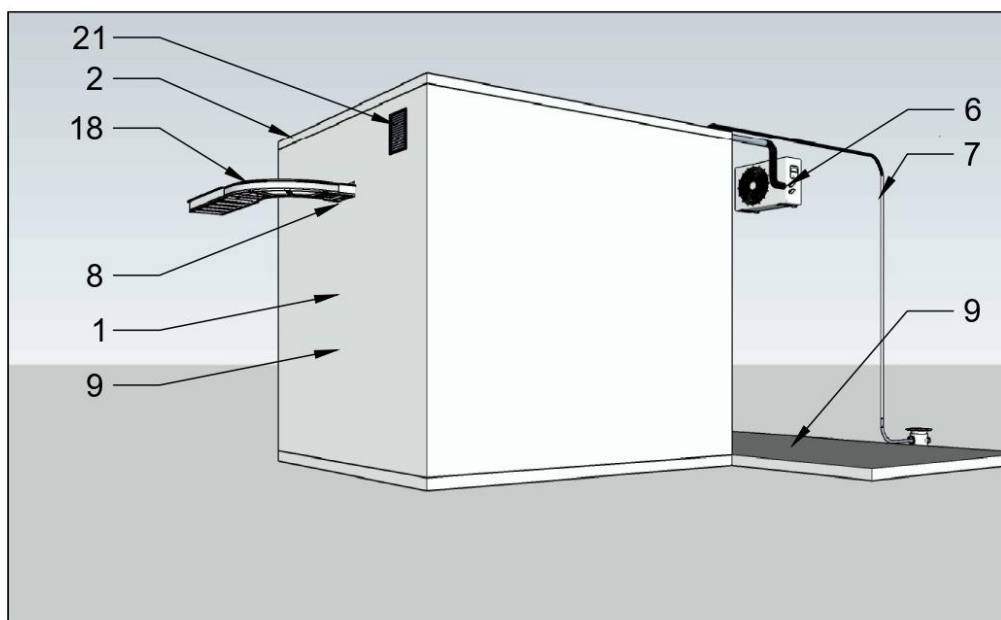


FIGURA 2 - VISTA POSTERIOR

- 1- Recinto resistente al fuego de sesenta minutos. (RF60)
Diseño y materiales deben proporcionar protección antivandálica, de acuerdo a nivel de seguridad requerido por la situación. Pisos, Paredes, cielorrasos, deberán sellarse, ser pintados y construidos con materiales que logren minimizar el polvo. Terminaciones de color claro para mejorar la iluminación de la Sala.
- 2- Cielorraso Rf60. Altura mínima: 2.60 m.
En caso de existir losa de hormigón armado, las paredes RF60 llegarán hasta la losa, a la que sólo se la en prolija y pinta. Se evitará la construcción del cielorraso. El Espacio deberá ser liberado de todo tipo de instalaciones preexistentes. De existir, se deberá eliminar caños de agua o desagües en el área de la sala segura.
- 6- Unidad exterior de AA sistema separado.
- 7- Desagüe de agua de condensación impulsada con bomba tipo Mini Orange Aspen Pumps según cálculo de altura y caudal, hasta desagües de la Inst. Sanitaria.
- 8- Acometida de instalaciones selladas con Sellador Elástico Hilti Cortafuego De Silicona Cp 601s
- 9- Pasillo semipúblico que permita el acceso directo del personal autorizado sin pasar por otros lugares restringido para acceder a la Sala Segura a cualquier hora.
- 10- Espacio previsto para ampliar el número de racks
- 18- Canalización según Normas de cableado estructurado y datacenters (ANSI/TIA 568, ANSI/TIA 569, ANSI/TIA 942). (1.5)
- 21- Rejilla de ventilación con extractor de aire automatizada con sistema de control de temperatura.

PROVINCIA DEL CHACO	SUBSECRETARÍA DE PLANIFICACIÓN Y PROYECTOS		PLANO N°:
M P E I	DIRECCION DE PROYECTOS		F2
OBRA: SALA SEGURA			ESCALA: S/E
UBICACION: -----			
PLANO: IMAGENES SALA SEGURA – VISTA POSTERIOR			FECHA 08/21
EQUIPO DE TRABAJO: RF/MS			

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

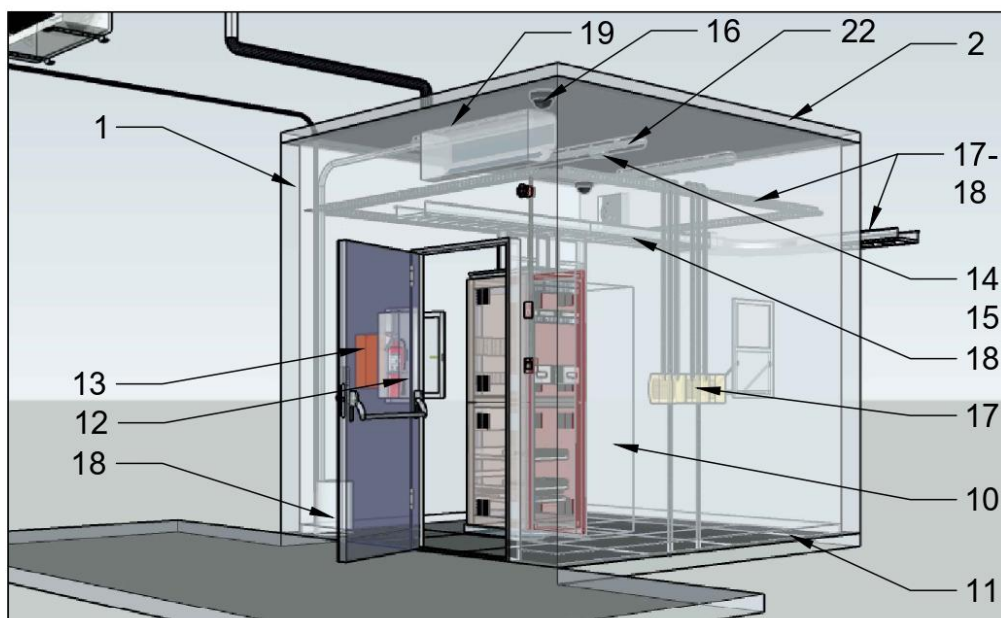


FIGURA 3 - VISTA TRANSPARENTE DEL INTERIOR

- 1- Recinto resistente al fuego de sesenta minutos. (RF60)
Diseño y materiales deben proporcionar protección antivandámica, de acuerdo a nivel de seguridad requerido por la situación. Pisos, Paredes, cielorrasos, deberán sellarse, ser pintados y contruidos con materiales que logren minimizar el polvo. Terminaciones de color claro para mejorar la iluminación de la Sala.
- 2- Cielorraso Rf60. Altura mínima: 2.60 m.
En caso de existir losa de hormigón armado, las paredes RF60 llegarán hasta la losa, a la que sólo se la enprolija y pinta. Se evitará la construcción del cielorraso. El Espacio deberá ser liberado de todo tipo de instalaciones preexistentes. De existir, se deberá eliminar caños de agua o desagües en el área de la sala segura.
- 10- Espacio previsto para ampliar el número de racks
- 11- Pisos con propiedades antiestáticas. Según apartado 1.1.3 del ANEXO I: Especificaciones para Salas Tecnológicas Seguras.
- 12- Matafuegos Haloclean (HCFC123) de 5 kg. Sello IRAM. Soporte, baliza y tarjeta.
- 13- Panel de Incendio Direccionable Inteligente con DACT (Comunicador / transmisor de alarma digital) telefónico e IP.
- 14- Detector de temperatura en el interior. 1.6.2
- 15- Detector de humo autónomo. 1.6.1
- 16- Dos cámaras de videovigilancia en el interior de la sala, en vértices opuestos. Videovigilancia con grabación 24/7 de la totalidad del interior de la STS.
- 17- Electricidad: alimentación exclusiva para dispositivos y servicios críticos de la sala y otra alimentación para servicios no críticos. (1.8). Prever la separación y disposición adecuada entre las puestas a tierra de los dispositivos electrónicos y la de los dispositivos eléctricos. 1.8
- 18- Canalización según Normas de cableado estructurado y datacenters (ANSI/TIA 568, ANSI/TIA 569, ANSI/TIA 942). (1.5)
- 19- Unidad de Aire Acondicionado Sistema Separado con potencia según cálculo. Frío solo. Ubicado sobre puerta para evitar goteos sobre instalaciones.

PROVINCIA DEL CHACO	SUBSECRETARIA DE PLANIFICACIÓN Y PROYECTOS		PLANO N°:
M P E I	DIRECCION DE PROYECTOS		F3
OBRA: SALA SEGURA			ESCALA: S/E
UBICACION: -----			
PLANO: IMAGENES SALA SEGURA – INTERIOR			FECHA 08/21
EQUIPO DE TRABAJO: RF/MS			

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

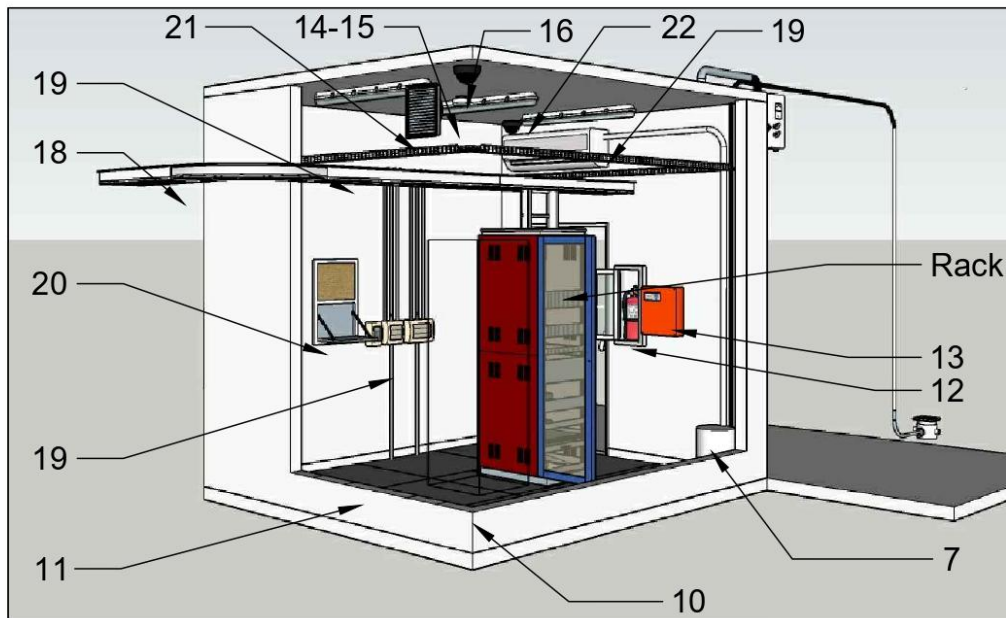


FIGURA 4 - VISTA DEL INTERIOR

- 7- Desagüe de agua de condensación impulsada con bomba tipo Mini Orange Aspen Pumps según cálculo de altura y caudal, hasta desagües de la Inst. Sanitaria.
- 8- Acometida de instalaciones selladas con Sellador Elástico Hilti Cortafuego De Silicona Cp 601s
- 10- Espacio previsto para ampliar el número de racks
- 11- Pisos con propiedades antiestáticas. Según apartado 1.1.3 del ANEXO I: Especificaciones para Salas Tecnológicas Seguras.
- 12- Matafuegos Haloclean (HCFC123) de 5 kg. Sello IRAM. Soporte, baliza y tarjeta.
- 13- Panel de Incendio Direccionable Inteligente con DACT (Comunicador / transmisor de alarma digital) telefónico e IP.
- 14- Detector de temperatura en el interior. 1.6.2
- 15- Detector de humo autónomo. 1.6.1
- 16- Dos cámaras de videovigilancia en el interior de la sala, en vértices opuestos. Videovigilancia con grabación 24/7 de la totalidad del interior de la STS.
- 17- Electricidad: alimentación exclusiva para dispositivos y servicios críticos de la sala y otra alimentación para servicios no críticos. (1.8). Prever la separación y disposición adecuada entre las puestas a tierra de los dispositivos electrónicos y la de los dispositivos eléctricos. 1.8
- 18- Canalización según Normas de cableado estructurado y datacenters (ANSI/TIA 568, ANSI/TIA 569, ANSI/TIA 942). (1.5)
- 19- Unidad de Aire Acondicionado Sistema Separado con potencia según cálculo. Frío solo. Instalado sobre puerta para evitar goteo sobre instalaciones.
- 20- Atril rebatible para apoyo Notebook y panel corcho para Instructivos de Uso Sala Tecnológicas Segura
- 21- Rejilla de ventilación con extractor de aire automatizada con sistema de control de temperatura.
- 22- Iluminación. 500 lux sobre el plano de trabajo. Artefacto

PROVINCIA DEL CHACO	SUBSECRETARIA DE PLANIFICACIÓN Y PROYECTOS		PLANO N°:
M P E I	DIRECCION DE PROYECTOS		F4
OBRA:	SALA SEGURA		ESCALA:
UBICACION:	-----		S/E
PLANO:	IMAGENES SALA SEGURA – INTERIOR		FECHA
EQUIPO DE TRABAJO:	RF/MS		08/21

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

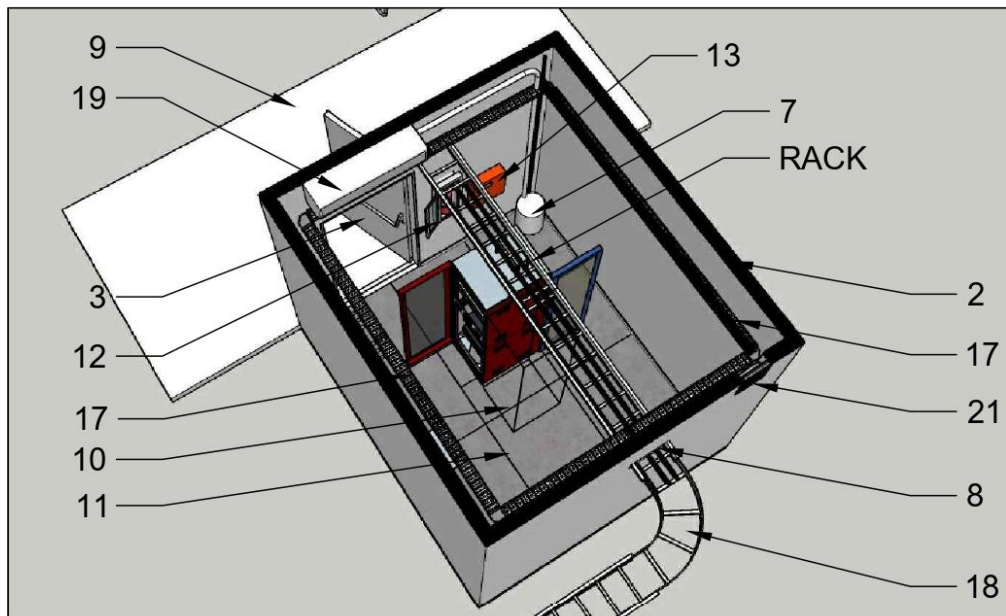


FIGURA 4 - VISTA DEL INTERIOR

- 1- Recinto resistente al fuego de sesenta minutos. (RF60)
Diseño y materiales deben proporcionar protección antivandálica, de acuerdo a nivel de seguridad requerido por la situación. Pisos, Paredes, cielorrasos, deberán sellarse, ser pintados y construidos con materiales que logren minimizar el polvo. Terminaciones de color claro para mejorar la iluminación de la Sala.
- 3- Puerta cortafuego Rf60 con homologación de INTI. Apertura hacia afuera. Doble contacto en sus cuatro lados, con burletes intumescentes. Dimensión mínima: 1.00 m por 2.05 m de alto. Cerradura reforzada del tipo doble tambor de bronce o biométrica como parte del sistema de control de acceso. Deberá garantizar una fácil apertura desde el exterior o interior, sin depender exclusivamente de mecanismo o sistemas electrónicos. Barral antipánico en el interior.
- 7- Desagüe de agua de condensación impulsada con bomba tipo Mini Orange Aspen Pumps según cálculo de altura y caudal, hasta desagües de la Inst. Sanitaria.
- 8- Acometida de instalaciones selladas con Sellador Elástico Hilti Cortafuego De Silicona Cp 601s
- 9- Pasillo semipúblico que permita el acceso directo del personal autorizado sin pasar por otros lugares restringido para acceder a la Sala Segura a cualquier hora.
- 10- Espacio previsto para ampliar el número de racks
- 11- Pisos con propiedades antiestáticas. Según apartado 1.1.3 del ANEXO I: Especificaciones para Salas Tecnológicas Seguras.
- 12- Matafuegos Haloclean (HCFC123) de 5 kg. Sello IRAM. Soporte, baliza y tarjeta.
- 13- Panel de Incendio Direccional Inteligente con DACT (Comunicador / transmisor de alarma digital) telefónico e IP.
- 17- Electricidad: alimentación exclusiva para dispositivos y servicios críticos de la sala y otra alimentación para servicios no críticos. (1.8). Prever la separación y disposición adecuada entre las puestas a tierra de los dispositivos electrónicos y la de los dispositivos eléctricos.
- 18- Canalización según Normas de cableado estructurado y datacenters (ANSI/TIA 568, ANSI/TIA 569, ANSI/TIA 942). (1.5)
- 19- Unidad de Aire Acondicionado Sistema Separado con potencia según cálculo. Frio solo. Instalado sobre puerta para evitar goteo sobre instalaciones.
- 21- Rejilla de ventilación con extractor de aire automatizada con sistema de control de temperatura.

PROVINCIA DEL CHACO	SUBSECRETARIA DE PLANIFICACIÓN Y PROYECTOS		PLANO N°:
M P E I	DIRECCION DE PROYECTOS		P5
OBRA:	SALA SEGURA		ESCALA:
UBICACION:	-----		S/E
PLANO:	IMAGENES SALA SEGURA		FECHA
EQUIPO DE TRABAJO:	RF/MS		08/21

Link para descarga de los planos (Acceso Público)

https://drive.google.com/drive/folders/12qbrbZgWek0qB9wvfNesTKvD_JPToD5_?usp=sharing

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Anexo VI: Riesgos de la Infraestructura Tecnológica de Casa de Gobierno

Estimación del Riesgo de la Infraestructura Tecnológica del Subsuelo de Casa de Gobierno						
Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A		A			
	M					
	B					
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Riesgo						
Riesgo		Probabilidad				
Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo						
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguardas implementadas
1	Servidores sin respaldo de datos	Crítico	Sin salvaguardas
2	Los servidores no cuentan con una protección energética (UPS)	Importante	Sin salvaguardas
3	Espacio físico no delimitado	Crítico	Sin salvaguardas
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del Subsuelo		Negativo	De 6 ítems considerados en el análisis, sólo 1 tiene implementada una salvaguarda, mientras que los 5 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica de la Planta Baja de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B		B			
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA					
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					
	A					
	M		M			
	B					
	MB					

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Riesgo		Probabilidad				
Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguadas implementadas
1	Servidores sin respaldo de datos	Apreciable	Backup manual en discos rígidos
2	Los servidores no cuentan con una protección energética (UPS)	Bajo	UPS
3	Espacio físico no delimitado	Apreciable	Cuarto de comunicaciones
4	Conexiones eléctricas deficientes	Apreciable	Línea eléctrica independiente
5	Cableado de red no documentado	Apreciable	Sin salvaguadas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos de la Planta Baja		Positivo	De 6 ítems considerados en el análisis, 5 tienen implementadas salvaguadas, mientras que sólo 1 no tiene ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del Entrepiso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A		A			
	M					
	B					
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguadas implementadas
1	Servidores sin respaldo de datos	Crítico	Sin salvaguadas
2	Los servidores no cuentan con una protección energética (UPS)	Importante	Sin salvaguadas
3	Espacio físico no delimitado	Crítico	Sin salvaguadas
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguadas
5	Cableado de red no documentado	Apreciable	Sin salvaguadas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del Entrepiso		Negativo	De 6 ítems considerados en el análisis, sólo 1 tiene implementada una salvaguarda, mientras que los 5 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 1º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					
	MB	MB				
Riesgo						
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					
	MB	MB				
Riesgo						
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo						
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					
Riesgo						
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvuardas implementadas
1	Servidores sin respaldo de datos	Despreciable	No contemplado
2	Los servidores no cuentan con una protección energética (UPS)	Despreciable	No contemplado
3	Espacio físico no delimitado	Crítico	Sin salvuardas
4	Conexiones eléctricas deficientes	Crítico	Sin salvuardas
5	Cableado de red no documentado	Apreciable	Sin salvuardas
6	Red no administrada	Bajo	Técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del 1º Piso		Negativo	De 4 ítems contemplados en el análisis, sólo 1 tiene implementada una salvaguarda, mientras que los 3 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 2º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B		B			
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguardas implementadas
1	Servidores sin respaldo de datos	Crítico	Sin salvaguardas
2	Los servidores no cuentan con una protección energética (UPS)	Bajo	UPS
3	Espacio físico no delimitado	Crítico	Sin salvaguardas
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del 2º Piso		Negativo	De 6 ítems considerados en el análisis, sólo 2 tienen implementadas salvaguardas, mientras que los 4 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 3º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					
	MB	MB				
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					
	MB	MB				
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguardas implementadas
1	Servidores sin respaldo de datos	Despreciable	No contemplado
2	Los servidores no cuentan con una protección energética (UPS)	Despreciable	No contemplado
3	Espacio físico no delimitado	Crítico	Sin salvaguardas
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del 3º Piso		Negativo	De 4 ítems contemplados en el análisis, sólo 1 tiene implementada una salvaguarda, mientras que los 3 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 4º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A		A			
	M					
	B					
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA					
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					
	A					
	M		M			
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

1	Servidores sin respaldo de datos	Apreciable	Backup manual en discos rígidos
2	Los servidores no cuentan con una protección energética (UPS)	Bajo	UPS
3	Espacio físico no delimitado	Apreciable	Cuarto de comunicaciones
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del 4º Piso		Positivo	De 6 ítems considerados en el análisis, sólo 4 tienen implementadas salvaguardas, mientras que los 2 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 5º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA					
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A		A			
	M					
	B					
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguardas implementadas
1	Servidores sin respaldo de datos	Apreciable	Backup automático en discos rígidos
2	Los servidores no cuentan con una protección energética (UPS)	Importante	Sin salvaguardas
3	Espacio físico no delimitado	Crítico	Sin salvaguardas
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco SA
Resultado de la estimación de riesgos del 5º Piso		Negativo	De 6 ítems considerados en el análisis, sólo 2 tienen implementadas salvaguardas, mientras que los 4 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 6º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A		A			
	M					
	B					
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA					
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguardas implementadas
1	Servidores sin respaldo de datos	Crítico	Sin salvaguardas
2	Los servidores no cuentan con una protección energética (UPS)	Importante	Sin salvaguardas
3	Espacio físico no delimitado	Apreciable	Cuarto de comunicaciones
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del 6º Piso		Negativo	De 6 ítems considerados en el análisis, sólo 2 tienen implementadas salvaguardas, mientras que los 4 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 7º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B		B			
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA					
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvuardas implementadas
1	Servidores sin respaldo de datos	Apreciable	Backup manual en discos rígidos
2	Los servidores no cuentan con una protección energética (UPS)	Bajo	UPS
3	Espacio físico no delimitado	Apreciable	Cuarto de comunicaciones
4	Conexiones eléctricas deficientes	Crítico	Sin salvuardas
5	Cableado de red no documentado	Apreciable	Sin salvuardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del 7º Piso		Positivo	De 6 ítems considerados en el análisis, 4 tienen implementadas salvuardas, mientras que 2 no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 8º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A		A			
	M					
	B					
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA					
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					MA
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguardas implementadas
1	Servidores sin respaldo de datos	Crítico	Sin salvaguardas
2	Los servidores no cuentan con una protección energética (UPS)	Importante	Sin salvaguardas
3	Espacio físico no delimitado	Apreciable	Cuarto de comunicaciones
4	Conexiones eléctricas deficientes	Crítico	Sin salvaguardas
5	Cableado de red no documentado	Apreciable	Sin salvaguardas
6	Red no administrada	Bajo	Personal interno que administra la red, además de los técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del 8º Piso		Negativo	De 6 ítems considerados en el análisis, sólo 2 tienen implementadas salvaguardas, mientras que los 4 restantes no tienen ninguna.

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Estimación del Riesgo de la Infraestructura Tecnológica del 9º Piso de Casa de Gobierno

Riesgo		Probabilidad				
Servidores sin respaldo de datos		MB	B	M	A	MA
Impacto	MA			MA		
	A					
	M					
	B					
	MB					
Riesgo		Probabilidad				
Los servidores no cuentan con una protección energética (UPS)		MB	B	M	A	MA
Impacto	MA					
	A		A			
	M					
	B					
	MB					
Riesgo		Probabilidad				
Espacio físico no delimitado		MB	B	M	A	MA
Impacto	MA					
	A					
	M			M		
	B					
	MB					
Riesgo		Probabilidad				
Conexiones eléctricas deficientes		MB	B	M	A	MA
Impacto	MA					
	A					
	M		M			
	B					
	MB					
Riesgo		Probabilidad				

"Procedimiento para la implementación de Salas Tecnológicas Seguras en organismos públicos en el marco de un Sistema de Cableado Estructurado. Caso de Estudio: Casa de Gobierno del Poder Ejecutivo de la Provincia del Chaco"

Cableado de red no documentado		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B					M
	MB					
Riesgo		Probabilidad				
Red no administrada		MB	B	M	A	MA
Impacto	MA					
	A					
	M					
	B			B		
	MB					

Ítem	Riesgo	Estimación del riesgo	Salvaguadas implementadas
1	Servidores sin respaldo de datos	Crítico	Sin salvaguadas
2	Los servidores no cuentan con una protección energética (UPS)	Importante	Sin salvaguadas
3	Espacio físico no delimitado	Apreciable	Cuarto de comunicaciones
4	Conexiones eléctricas deficientes	Apreciable	Línea eléctrica independiente
5	Cableado de red no documentado	Apreciable	Sin salvaguadas
6	Red no administrada	Bajo	Técnicos de la empresa Ecom Chaco S.A.
Resultado de la estimación de riesgos del 9º Piso		Negativo	De 6 ítems considerados en el análisis, sólo 3 tienen implementadas salvaguadas, mientras que los 3 restantes no tienen ninguna.

Link para descarga de las estimaciones de riesgos por piso (Acceso Público)

<https://drive.google.com/drive/folders/1IRMsEBq1xhGPJR8aCScXSn4KeMtV6mSM?usp=sharing>