Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gerencia de Sistemas

Tema: Diseño de un modelo de ciberseguridad basado en el marco de ciberseguridad v1.1 de la NIST alineado a COBIT 2019, para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones. Caso de estudio Área de Transmisiones – Corporación Nacional de Telecomunicaciones

Autor: Tipan Oscullo Dario Javier

Director: Msc. Pinto Auz, Diego Julián

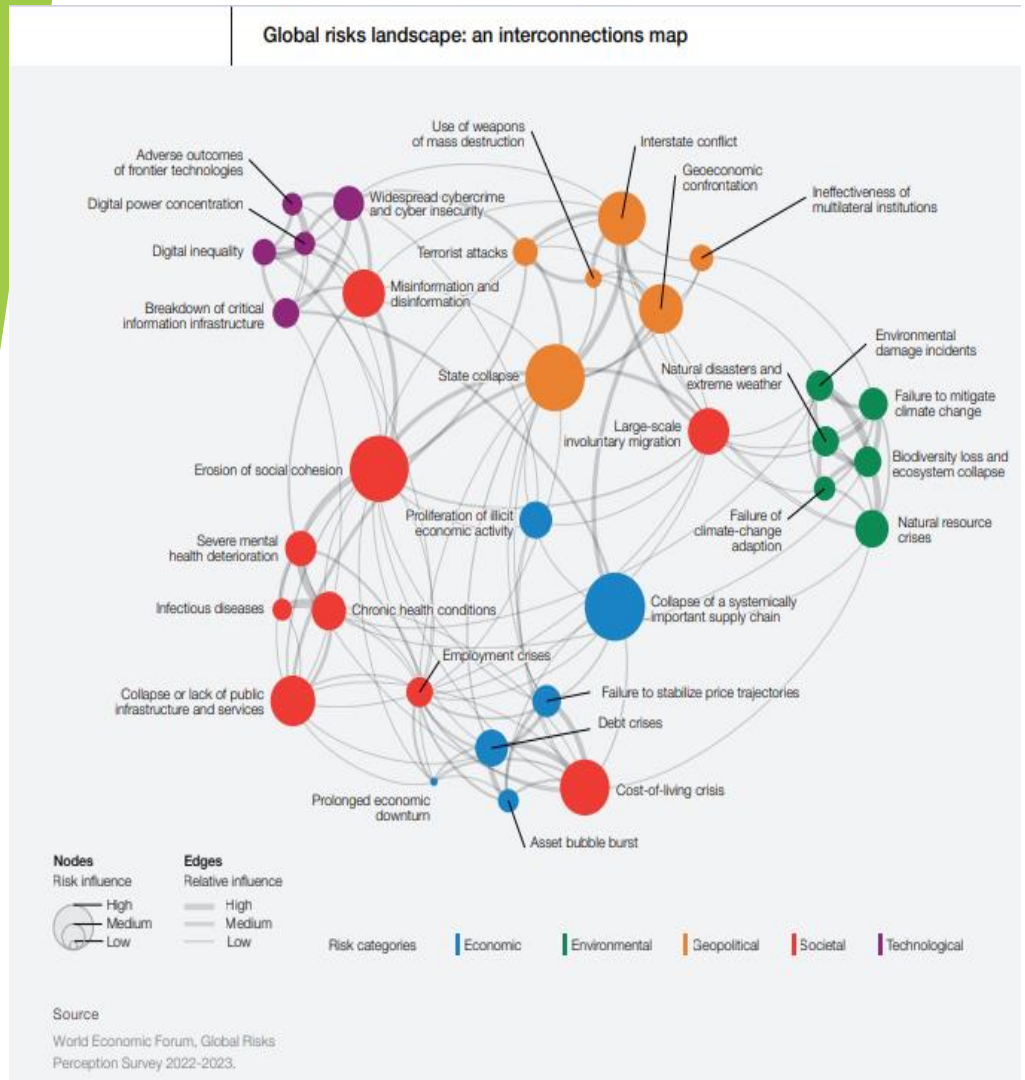
Sangolquí - 2023


la ciberseguridad no es sólo responsabilidad
del departamento informático,
sino de todos.
—Frank Abagnale.

CONTENIDO

- ANTECEDENTES
- PLANTEAMIENTO PROBLEMA
- HIPOTESIS
- OBJETIVO
- ANALISIS DE RIESGOS
- DISEÑO DEL MODELO DE CIBERSEGURIDAD
- CONCLUSIONES Y RECOMENDACIONES

Antecedentes

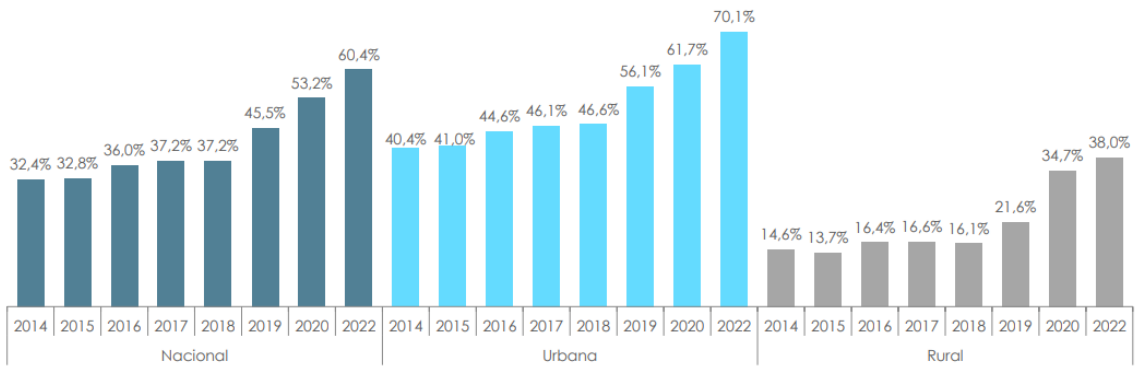


1	Failure to mitigate climate change
2	Failure of climate-change adaption
3	Natural disasters and extreme weather events
4	Biodiversity loss and ecosystem collapse
5	Large-scale involuntary migration
6	Natural resource crises
7	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity
9	Geoeconomic confrontation
10	Large-scale environmental damage incidents
11	Misinformation and disinformation
12	Ineffectiveness of multilateral institutions and international cooperation
13	Interstate conflict
14	Debt crises
15	Cost-of-living crisis
16	Breakdown of critical information infrastructure

INEC Buenas cifras, mejores vidas

Hogares con acceso a internet

Nacional y Área(Urbana/Rural)



INDICADORES

Índice global de Ciberseguridad: La UIT mide el compromiso en ciberseguridad para fomentar una cultura global. Se mide cada 2 años.

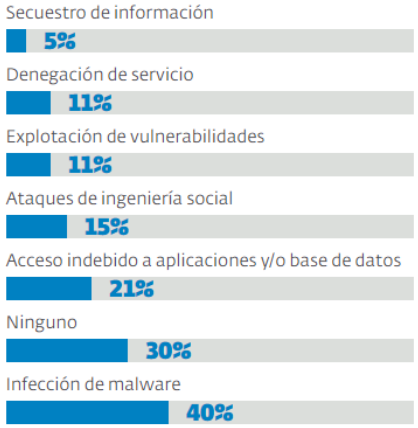
	Resultado 2020	Resultado 2021	Meta 2022	Meta 2024
Índice global de Ciberseguridad	26.3	30	35.3	51.3

Datos de la región en el índice de ciberseguridad

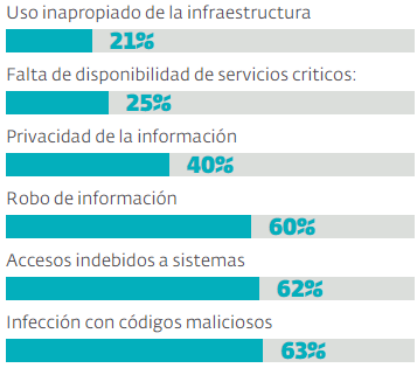
- Perú 56
- Colombia 64
- Argentina 48

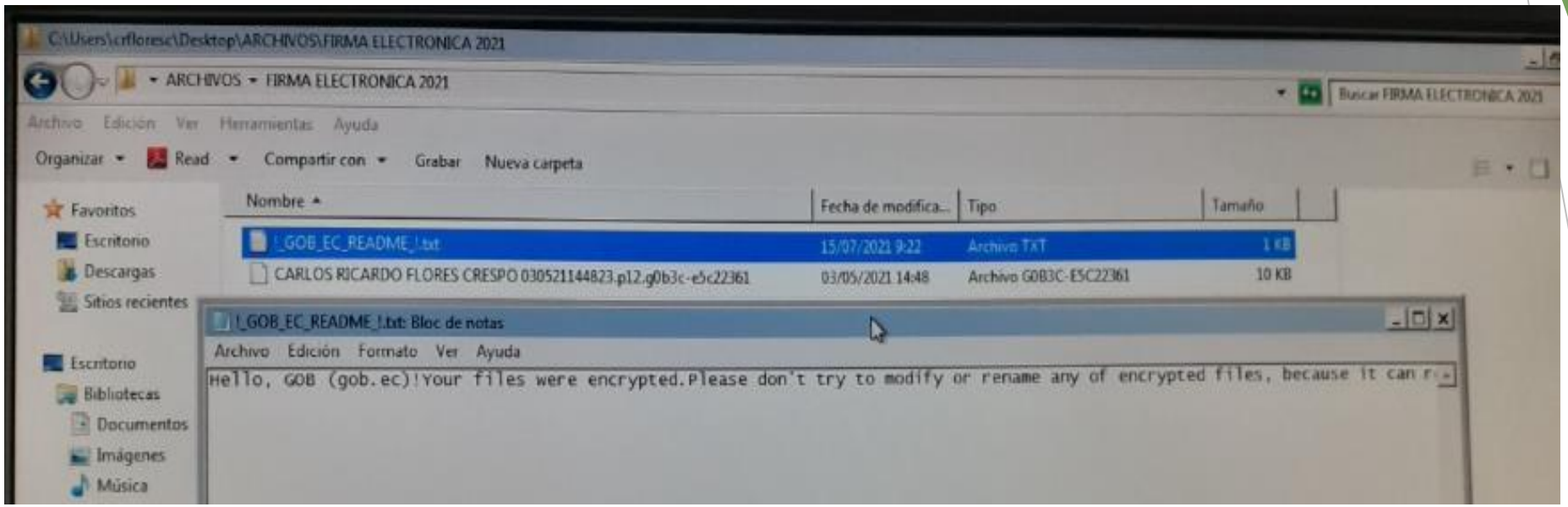
En Latinoamérica Ecuador

Incidentes ocurridos en los últimos 12 meses



Preocupaciones de seguridad




C:\Users\crfloresc\Desktop\ARCHIVOS\FIRMA ELECTRONICA 2021
ARCHIVOS ▸ FIRMA ELECTRONICA 2021
Buscar FIRMA ELECTRONICA 2021
Archivo Edición Ver Herramientas Ayuda
Organizar Read Compartir con Grabar Nueva carpeta
Favoritos
Escritorio
Descargas
Sitios recientes
Escritorio
Bibliotecas
Documentos
Imágenes
Música
Nombre
Fecha de modifica...
Tipo
Tamaño
!_GOB_EC_README_!.txt
15/07/2021 9:22
Archivo TXT
1 KB
CARLOS RICARDO FLORES CRESPO 030521144823.p12.g0b3c-e5c22361
03/05/2021 14:48
Archivo G0B3C-E5C22361
10 KB
!_GOB_EC_README_!.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
Hello, GOB (gob.ec)!Your files were encrypted.Please don't try to modify or rename any of encrypted files, because it can r

Planteamiento del Problema

En el país, la CNT a través de su plataforma tecnológica de transmisión interconecta y provee servicios para instituciones del estado ecuatoriano, ejército, policía nacional, unidades educativas públicas e infocentros, convirtiéndose así en una infraestructura critica digital. La protección de esta plataforma es escasa, en razón de que no cuenta con un modelo de ciberseguridad alineado a la estrategia empresarial que permita mantener la disponibilidad de interconexión y conectividad.

Hipótesis

Si se diseñara un modelo de ciberseguridad utilizando un marco de ciberseguridad alineado a un marco de gobierno y gestión, se podría determinar perfiles de ciberseguridad en los cuales los procesos y controles tengan relación directa con los objetivos empresariales.

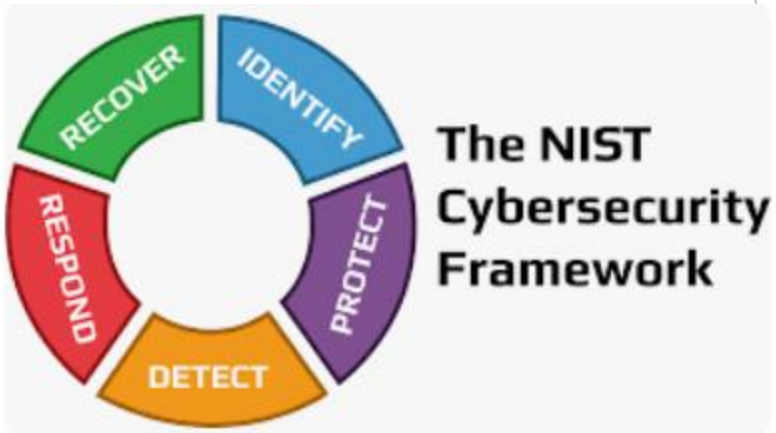
Objetivo

Realizar el diseño de un modelo de ciberseguridad basado en el marco de ciberseguridad v1.1 para infraestructuras críticas de la NIST alineado a COBIT 2019 para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones, teniendo como caso de estudio al Área de Transmisiones de la Corporación Nacional de Telecomunicaciones

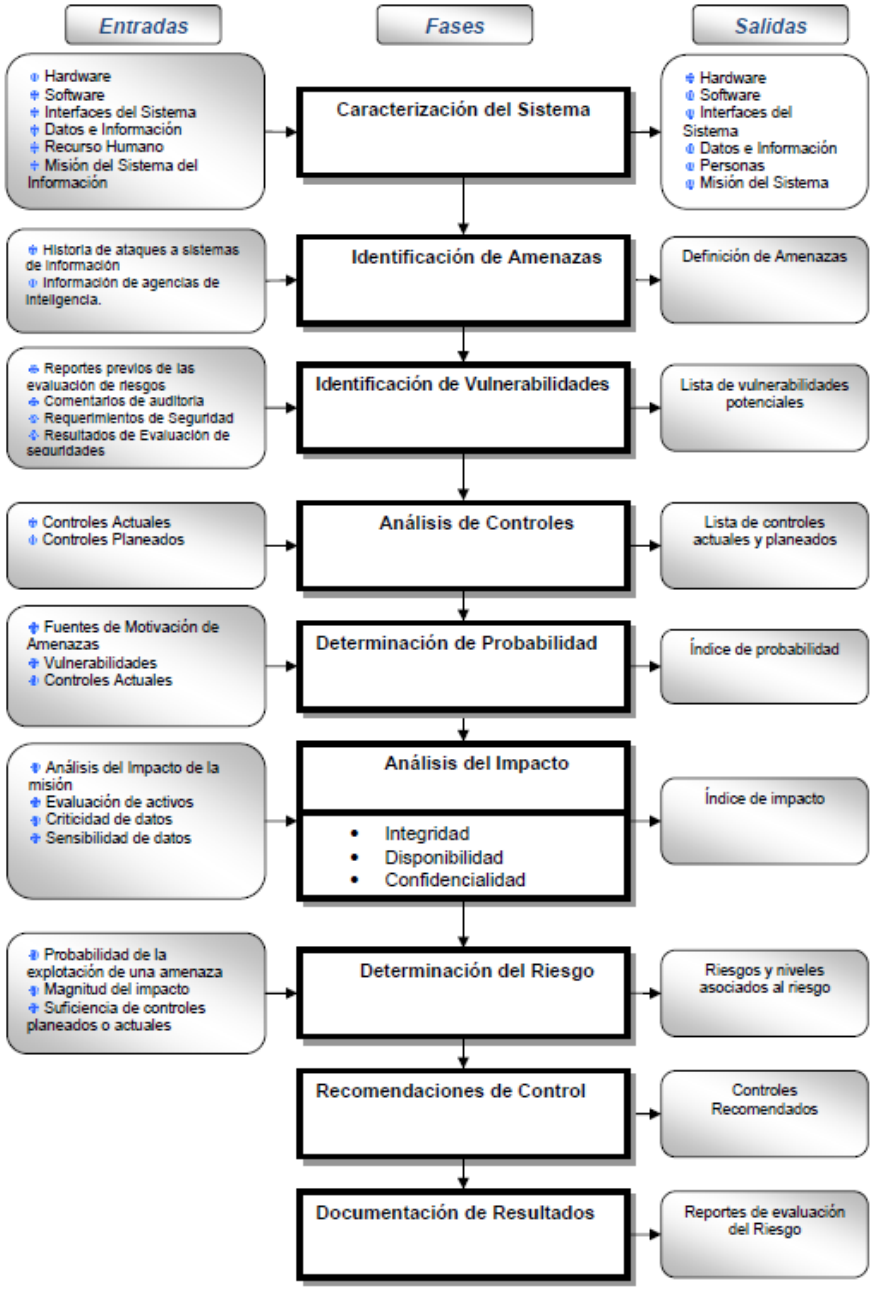
.

Marcos de trabajo aplicados

COBIT 2019



Análisis de Riesgos NIST SP 800-30



Análisis de Riesgos Caracterización del Sistema

Grupo de Activo	Tipo de Activo	Descripción	Identificación
Primario	Dato	Información que se maneja en el área	INFO
Soporte	Tecnología	Hardware donde se procesa la información	HW
Soporte	Aplicación	Software que se utiliza para dar soporte a los procesos	SW
Soporte	Instalación	Lugar donde se encuentran los activos de información	INS
Soporte	Personal	Analistas que manejan los activos	PER
Soporte	Servicio	Servicios que brinda el área	SERV
Soporte	Redes	Interconexión con la red interna y externa	NET

Análisis de Riesgos Identificación de amenzas

Tipo	Identificación	Descripción
Adversa	AD	Individuos, grupos, organizaciones o países buscan explotar la dependencia de la organización sobre los recursos cibernéticos.
Accidental	A	Acciones erróneas realizadas por el personal de la empresa sobre los activos al ejecutar sus actividades diarias.
Estructural	E	Falla de equipos, controles ambientales o software debido a el envejecimiento, agotamiento de recursos u otras, que exceden los parámetros óptimos.
Ambiente	AMB	Desastres naturales y fallas en los servicios de infraestructuras críticas de los cuales la empresa depende para su funcionamiento

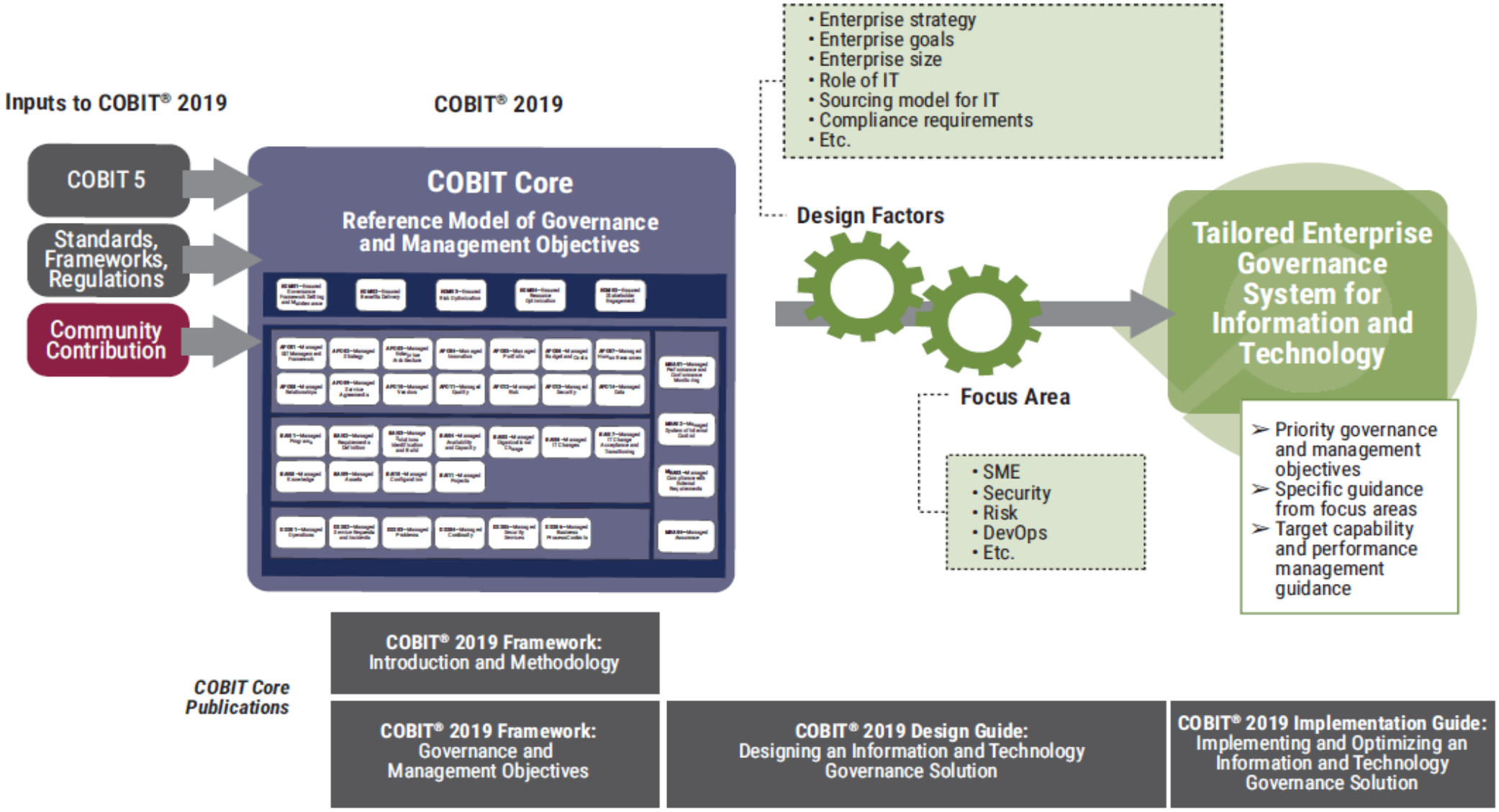
Análisis de Riesgos Impacto

Nivel de Impacto	Descripción
Alto	El evento de amenaza puede resultar en tener un efecto adverso severo en las operaciones, activos entre otros, esto se traduce en pérdida de la capacidad de la misión en una medida y duración que la organización no puede realizar sus funciones principales, provocar daños importantes en los activos y resultar en una pérdida financiera importante.
Medio	El evento de amenaza puede resultar en tener un efecto adverso serio en las operaciones, activos entre otros, esto se traduce en degradación de la capacidad de la misión en una medida y duración que la organización puede realizar sus funciones principales, pero la efectividad de las funciones se reduce significativamente y provocar daños significativos en los activos y resultar en una pérdida financiera significativa.
Bajo	El evento de amenaza puede resultar en tener un efecto adverso limitado en las operaciones, activos entre otros, esto se traduce en degradación de la capacidad de la misión en una medida y duración que la organización puede realizar sus funciones principales, pero la efectividad de las funciones se reduce notablemente y ocasionar daños menores en los activos y resultar en una pérdida financiera significativa.

Análisis de Riesgos
Mapa de calor riesgos

		Nivel de Impacto		
		Bajo	Medio	Alto
PROBABILIDAD	Alto	Aceptable	Moderado	Inaceptable
	Medio	Aceptable	Moderado	Moderado
	Bajo	Aceptable	Aceptable	Moderado

Diseño del Modelo



Diseño del Modelo

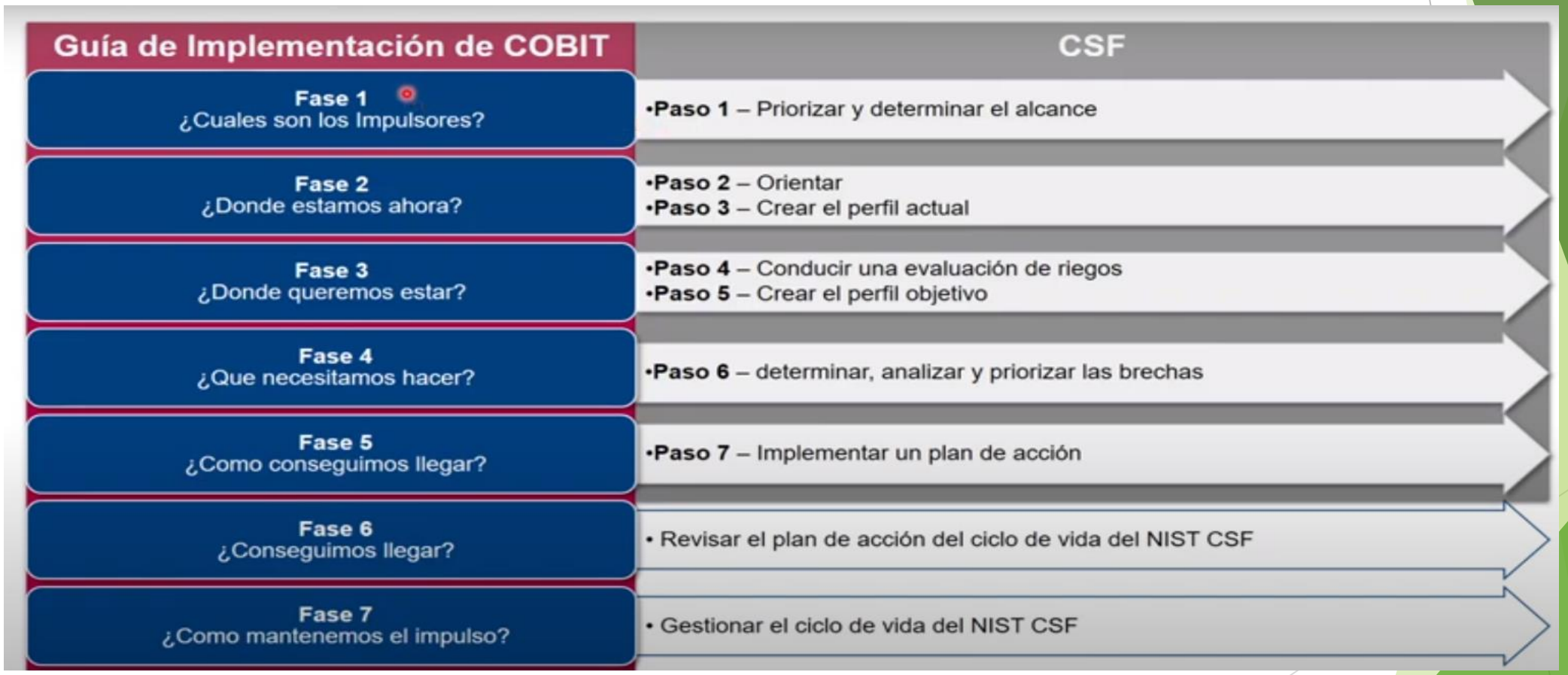
Diseño del Modelo

Figure 2.6—Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, USA, 16 April 2018, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf*

Diseño del Modelo



Priorización y Alcance

Id FD	Factor de Diseño	Justificación
FD1	Estrategia Empresarial	Es necesario expresar la estrategia de la CNT en uno o varios arquetipos de estrategia propuestos de Cobit 2019 para optimizar el riesgo cibernético.
FD2	Metas Empresariales	Es fundamental determinar los objetivos alineados a Cobit 2019 que sirvan de soporte para alcanzar la estrategia empresarial
FD3	Perfil de Riesgo	Es importante identificar al tipo de riesgo al que está expuesta el área y verificar si esta dispuestas a alcanzar sus objetivos a pesar del margen de riesgo.

Priorización y Alcance

Value	Importance (1-5)	Baseline
Growth/Acquisition	3	3
Innovation/Differentiation	5	3
Cost Leadership	2	3
Client Service/Stability	4	3

DF1	Growth / Acquisition	Innovation / Differentiation	Cost Leadership	Client Service / Stability
EDM01	1.0	2.0	1.5	2.0
EDM02	2.0	2.0	2.0	3.5
EDM03	3.0	4.0	2.0	3.0
EDM04	1.5	2.0	4.0	1.0
EDM05	1.5	1.5	1.0	2.0
APO01	1.0	1.0	1.0	1.0
APO02	2.5	3.5	1.5	1.0
APO03	3.0	2.0	1.0	1.0
APO04	2.0	4.0	1.0	1.0
APO05	2.0	4.0	2.5	1.0
APO06	2.0	1.0	4.0	1.0
APO07	2.0	3.0	1.0	1.0
APO08	1.0	1.5	1.0	3.5
APO09	3.0	3.0	1.5	4.0
APO10	2.0	2.0	3.5	1.5
APO11	2.0	1.0	1.0	4.0
APO12	3.0	2.5	1.0	2.5
APO13	4.0	4.0	1.0	3.0
APO14	4.0	3.0	1.0	1.0
BAI01	2.0	2.0	1.5	1.5
BAI02	2.0	1.0	1.5	1.0
BAI03	2.5	2.5	1.5	1.0
BAI04	2.0	2.0	1.0	3.0
BAI05	1.0	1.0	1.0	1.5
BAI06	2.0	2.0	1.0	1.5
BAI07	1.5	2.0	1.0	1.5
BAI08	3.0	3.5	1.0	1.0
BAI09	2.0	3.0	1.0	2.5
BAI10	3.0	2.5	1.0	3.0
BAI11	3.0	3.0	1.5	1.0

Priorización y Alcance

Dominio	Objetivos Cobit 2019	Descripción	Calificación
Evaluar, Dirigir y Supervisar	EDM02	Asegurar la obtención de beneficios	34
	EDM03	Asegurar la optimización del riesgo	45
Alinear, Planear y Organizar	APO04	Gestionar la innovación	36
	APO09	Gestionar los acuerdos de servicios	43
	APO12	Gestionar el riesgo	33.5
	APO13	Gestionar la seguridad	46
	APO14	Gestionar los datos	33
Construir, Adquirir e Implementar	BAI08	Gestionar el conocimiento	36.5
	BAI09	Gestionar los activos	33
	BAI10	Gestionar la configuración	40
Entrega, Servicio y Soporte.	DSS04	Gestionar la continuidad	33.5
	DSS05	Gestionar los servicios de seguridad	36

Priorización y Alcance

Id OE	Objetivo Estratégico	Dimensiones Cobit 2019
OE1	Incrementar la cobertura y la base de clientes en las líneas de negocio de la empresa	Cliente / Interna
OE2	Incrementar la conectividad de los ciudadanos mediante los servicios que brinda la CNT, tomando en cuenta la planificación territorial.	Cliente / Interna
OE3	Incrementar la participación y competitividad de la CNT como principal proveedor de telecomunicaciones y TICs en el sector privado y público.	Cliente
OE4	Incrementar productos y servicios de telecomunicaciones innovadores, convergentes, de calidad, seguros y con excelencia al cliente, desarrollando capacidades digitales que impulsen la constante transformación	Interna
OE5	Mantener el talento humano altamente capacitado, competente y comprometido con la organización.	Aprendizaje y Crecimiento
OE6	Incrementar la rentabilidad y crecimiento de ingresos de las líneas de negocio, asegurando la sostenibilidad financiera de la empresa.	Financiera

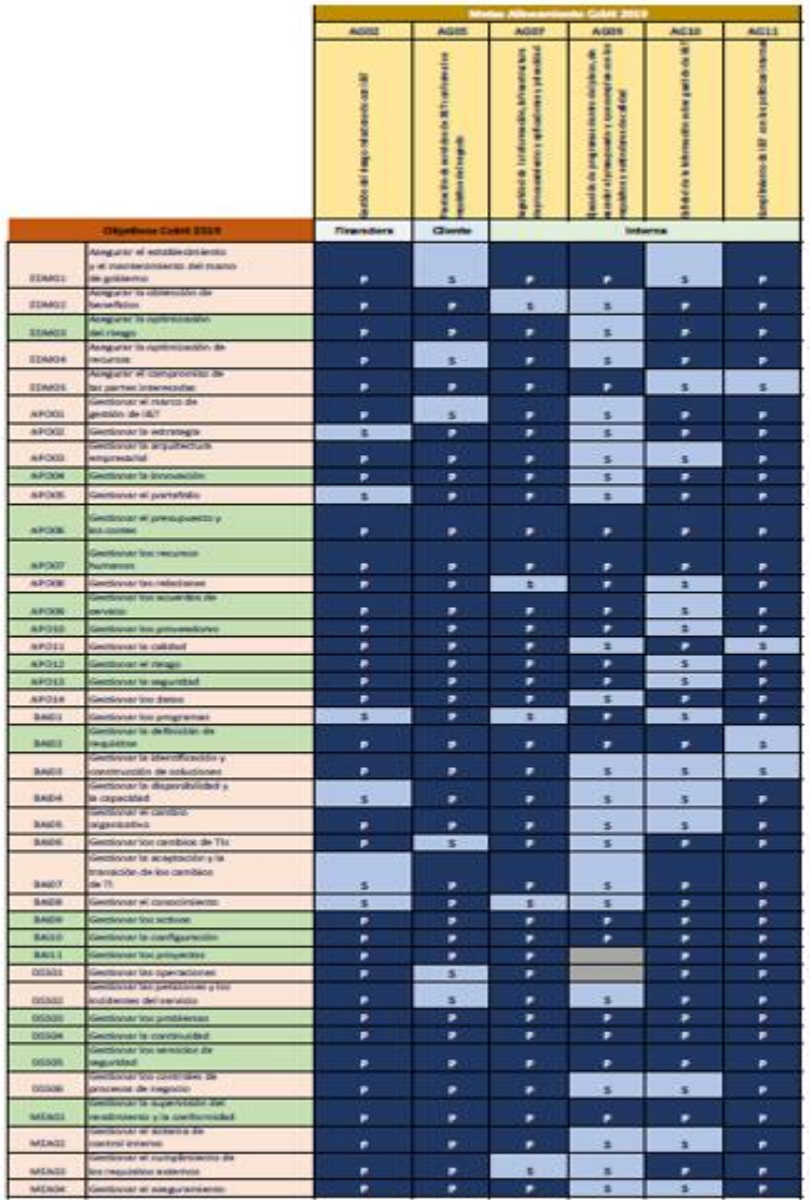
Priorización y Alcance

	Metas Empresariales Cobit 2019												
	EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
	Portafolio de productos y servicios competitivos	Gestión del riesgo del negocio	Cumplimiento de leyes y regulaciones externas	Calidad de la información financiera	Cultura del servicio orientado al cliente	Continuidad y disponibilidad del servicio del negocio	Calidad de la información sobre gestión	Optimización de la funcionalidad de los procesos internos de negocio	Optimización de costes de los procesos de negocio	Habilidades, motivación y productividad del personal	Cumplimiento con las políticas internas	Gestión de programas de transformación digital	Innovación de productos y negocios
Objetivos CNT	Financiera				Cliente			Interna				Crecimiento	
OE1	S	P	P	S	S	P	P	P	S	S	P	P	P
OE2	S	P	P	S	P	P	P	P	S	S	P	P	P
OE3	P	P	P	S	S	P	S	S	S	S	P	P	S
OE4	P	P	P	S	P	P	S	P	S	S	P	P	P
OE5		S	S			S	S	S		P	S	P	S
OE6		P	P	P	S	S	S	S	P	S	P	S	S

Priorización y Alcance

		Metas Alineamiento Cobit 2019												
		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		Cumplimiento y soporte de I&T para el cumplimiento del negocio con leyes y regulaciones externas	Gestión del riesgo relacionado con I&T	Beneficios obtenidos del portafolio de inversiones y servicios habilitados por I&T	Calidad de la información financiera relacionada con la tecnología	Prestación de servicios de I&T conforme los requisitos del negocio	Agilidad para convertir los requisitos del negocio en soluciones operativas	Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad	Habilidad y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	Ejecución de programas dentro del plazo, sin exceder el presupuesto y que cumplen con los requisitos y estándares de calidad	Calidad de la información sobre gestión de I&T	Cumplimiento de I&T con las políticas internas	Personal competente y motivado con un entendimiento de la tecnología y negocio	Conocimiento, experiencia e iniciativas para la innovación empresarial
Metas Empresariales Cobit 2019		Financiera				Cliente		Interna					Crecimiento	
EG02	Gestión del riesgo del negocio	P	P	S	S	P	S	P	P	P	P	P	P	P
EG03	Cumplimiento de leyes y regulaciones externas	P	P	P	S	P	S	S		S	S	S		S
EG06	Continuidad y disponibilidad del servicio del negocio	P	P	P	S	P	S	P	S	P	P	P	P	S
EG11	Cumplimiento con las políticas internas		S	S	P	S	S	P	P	P	P	P	S	P
EG12	Gestión de programas de transformación digital	S	P	P	S	P	P	P	P	P	P	P	S	P

Priorización y Alcance



Objetivos Cobit 2019		Financiera	Cliente	Interna			
		AG02	AG05	AG07	AG09	AG10	AG11
EDM01	Asegurar el establecimiento y el mantenimiento del marco de gobierno	P	S	P	P	S	P
EDM02	Asegurar la obtención de beneficios	P	P	S	S	P	P
EDM03	Asegurar la optimización del riesgo	P	P	P	S	P	P
EDM04	Asegurar la optimización de recursos	P	S	P	S	P	P
EDM05	Asegurar el compromiso de las partes interesadas	P	P	P	P	S	S
APO01	Gestionar el marco de gestión de I&T	P	S	P	S	P	P
APO02	Gestionar la estrategia	S	P	P	S	P	P
APO03	Gestionar la arquitectura empresarial	P	P	P	S	S	P
APO04	Gestionar la innovación	P	P	P	S	P	P
APO05	Gestionar el portafolio	S	P	P	S	P	P
APO06	Gestionar el presupuesto y los costes	P	P	P	P	P	P
APO07	Gestionar los recursos humanos	P	P	P	P	P	P
APO08	Gestionar las relaciones	P	P	S	P	S	P
APO09	Gestionar los acuerdos de servicio	P	P	P	P	S	P
APO10	Gestionar los proveedores	P	P	P	P	S	P
APO11	Gestionar la calidad	P	P	P	S	P	S
APO12	Gestionar el riesgo	P	P	P	P	S	P
APO13	Gestionar la seguridad	P	P	P	P	S	P
APO14	Gestionar los datos	P	P	P	S	P	P
BAI01	Gestionar los programas	S	P	S	P	S	P
BAI02	Gestionar la definición de requisitos	P	P	P	P	P	S
BAI03	Gestionar la identificación y construcción de soluciones	P	P	P	S	S	S
BAI04	Gestionar la disponibilidad y la capacidad	S	P	P	S	S	P
BAI05	Gestionar el cambio organizativo	P	P	P	S	S	P
BAI06	Gestionar los cambios de TI	P	S	P	S	P	P
BAI07	Gestionar la aceptación y la transición de los cambios de TI	S	P	P	S	P	P
BAI08	Gestionar el conocimiento	S	P	S	S	P	P
BAI09	Gestionar los activos	P	P	P	P	P	P
BAI10	Gestionar la configuración	P	P	P	P	P	P
BAI11	Gestionar los proyectos	P	P	P		P	P
DSS01	Gestionar las operaciones	P	S	P		P	P
DSS02	Gestionar las peticiones y los incidentes del servicio	P	S	P	S	P	P
DSS03	Gestionar los problemas	P	P	P	P	P	P
DSS04	Gestionar la continuidad	P	P	P	P	P	P
DSS05	Gestionar los servicios de seguridad	P	P	P	P	P	P
DSS06	Gestionar los controles de procesos de negocio	P	P	P	S	S	P
MEA01	Gestionar la supervisión del rendimiento y la conformidad	P	P	P	P	P	P
MEA02	Gestionar el sistema de control interno	P	P	P	S	S	P
MEA03	Gestionar el cumplimiento de los requisitos externos	P	P	S	S	P	P
MEA04	Gestionar el aseguramiento	P	P	P	S	S	P

Priorización y Alcance

Objetivos Gobierno y Gestión COBIT 2019 FD2

Objetivos Cobit 2019	Descripción
EDM03	Asegurar la optimización del riesgo
APO04	Gestionar la innovación
APO06	Gestionar el presupuesto y los costes
APO07	Gestionar los recursos humanos
APO09	Gestionar los acuerdos de servicio
APO10	Gestionar los proveedores
APO12	Gestionar el riesgo

Objetivos Cobit 2019	Descripción
APO13	Gestionar la seguridad
BAI02	Gestionar la definición de requisitos
BAI09	Gestionar los activos
BAI10	Gestionar la configuración
BAI11	Gestionar los proyectos
DSS03	Gestionar los problemas
DSS04	Gestionar la continuidad
DSS05	Gestionar los servicios de seguridad
MEA01	Gestionar la supervisión del rendimiento y conformidad

Priorización y Alcance

DF3	RISKCAT01 IT Investment Decision Making, Portfolio Definition & Maintenance	RISKCAT02 Program & Projects Life Cycle Management	RISKCAT03 IT Cost & Oversight	RISKCAT04 IT Expertise, Skills & Behavior	RISKCAT05 Enterprise/ IT Architecture	RISKCAT06 IT Operational Infrastructure Incidents	RISKCAT07 Unauthorized Actions	RISKCAT08 Software Adoption/ Usage Problems	RISKCAT09 Hardware Incidents	RISKCAT10 Software Failures	RISKCAT11 Logical Attacks (Hacking, Malware, etc.)	RISKCAT12 Third-Party/ Supplier Incidents	RISKCAT13 Noncompliance	RISKCAT14 Geopolitical Issues	RISKCAT15 Industrial Action	RISKCAT16 Acts of Nature	RISKCAT17 Technology-Based Innovation	RISKCAT18 Environmental	RISKCAT19 Data & Information Management
EDM01	3.0	2.0	3.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	3.0	2.0	0.0	0.0	2.0	2.0	2.0
EDM02	3.0	2.0	0.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	3.0	1.0	3.0
EDM03	2.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	2.0	0.0	3.0	3.0	0.0	0.0	0.0	2.0	3.0
EDM04	3.0	0.0	4.0	3.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	1.0	0.0	2.0	0.0	0.0	2.0	3.0
EDM05	3.0	1.0	3.0	0.0	0.0	0.0	2.0	0.0	0.0	1.0	0.0	1.0	3.0	3.0	0.0	0.0	0.0	2.0	2.0
APO01	2.0	3.0	2.0	0.0	2.0	2.0	4.0	2.0	0.0	2.0	3.0	3.0	3.0	0.0	0.0	0.0	3.0	2.0	3.0
APO02	2.0	0.0	0.0	0.0	3.0	0.0	0.0	2.0	1.0	0.0	1.0	2.0	0.0	0.0	0.0	0.0	2.0	2.0	1.0
APO03	2.0	0.0	0.0	0.0	4.0	0.0	0.0	2.0	0.0	2.0	2.0	2.0	0.0	0.0	0.0	0.0	2.0	0.0	3.0
APO04	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	4.0	0.0	0.0
APO05	4.0	2.0	2.0	0.0	2.0	0.0	0.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0
APO06	2.0	3.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	2.0	0.0	0.0	2.0	2.0	0.0
APO07	0.0	0.0	0.0	4.0	0.0	2.0	3.0	3.0	0.0	0.0	2.0	0.0	0.0	2.0	4.0	0.0	2.0	2.0	0.0
APO08	0.0	0.0	0.0	2.0	2.0	0.0	0.0	4.0	0.0	0.0	2.0	2.0	0.0	0.0	0.0	0.0	3.0	0.0	2.0
APO09	0.0	0.0	2.0	0.0	0.0	0.0	2.0	3.0	0.0	1.0	2.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
APO10	0.0	2.0	3.0	0.0	0.0	0.0	2.0	2.0	3.0	2.0	2.0	4.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0
APO11	0.0	3.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0
APO12	0.0	0.0	0.0	0.0	0.0	0.0	3.0	0.0	0.0	2.0	3.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0
APO13	0.0	0.0	0.0	0.0	0.0	0.0	4.0	0.0	0.0	0.0	4.0	0.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0
APO14	0.0	0.0	0.0	0.0	0.0	0.0	3.0	2.0	0.0	0.0	2.0	0.0	3.0	0.0	2.0	4.0	2.0	0.0	4.0
BAI01	0.0	4.0	0.0	0.0	2.0	0.0	0.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI02	2.0	2.0	0.0	0.0	2.0	0.0	0.0	3.0	0.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI03	0.0	3.0	0.0	0.0	2.0	0.0	0.0	2.0	0.0	3.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI04	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI05	0.0	2.0	0.0	2.0	0.0	0.0	0.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI06	0.0	0.0	0.0	0.0	0.0	3.0	4.0	0.0	0.0	2.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	3.0
BAI07	0.0	0.0	0.0	0.0	0.0	2.0	3.0	2.0	0.0	4.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI08	0.0	0.0	0.0	2.0	0.0	3.0	0.0	3.0	0.0	3.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0	2.0

Priorización y Alcance

Dominio	Objetivos Cobit 2019	Descripción
Evaluar, Dirigir y Supervisar	EDM03	Asegurar la optimización del riesgo
Alinear, Planear y Organizar	APO06	Gestionar el presupuesto y los costes
	APO07	Gestionar los recursos humanos
	APO09	Gestionar los acuerdos de servicio
	APO10	Gestionar los proveedores
	APO12	Gestionar el riesgo
	APO13	Gestionar la seguridad
	APO14	Gestionar los datos
Construir, Adquirir e Implementar	BAI09	Gestionar los activos
Entrega, Servicio y Soporte.	DSS04	Gestionar la continuidad

Priorización y Alcance

Dominio	DF1	DF2	DF3	Prioritarios
Evaluar, Dirigir y Supervisar	EDM02			No
	EDM03	EDM03	EDM03	Si
Alinear, Planear y Organizar	APO04	APO04		No
		APO06	APO06	No
		APO07	APO07	No
	APO09	APO09	APO09	Si
		APO10	APO10	No
	APO12	APO12	APO12	Si
	APO13	APO13	APO13	Si
	APO14		APO14	No
Construir, Adquirir e Implementar		BAI02		No
	BAI08			No
	BAI09	BAI09	BAI09	Si
	BAI10	BAI10		No
		BAI11		No
		DSS03		No
Entrega, Servicio y Soporte.	DSS04	DSS04	DSS04	Si
	DSS05	DSS05		No

Orientación y Perfil Actual

Abbreviation	Description	% Achieved
N	Not achieved	0 to ≤15%
P	Partially achieved	> 15% to ≤50%
L	Largely achieved	> 50% to ≤85%
F	Fully achieved	> 85% to ≤100%

Perfil Actual Función Identificar

Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	Nivel Implementación				Promedio
					N	P	L	F	
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	ID.AM-1	Los dispositivos y sistemas físicos dentro de la organización están inventariados.	BAI09.01			55		57,5
				BAI09.02			60		
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	ID.AM-2	Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	BAI09.05		47			47
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	ID.AM-4	Los sistemas de información externos están catalogados.	APO02.02		35			39
				APO10.01		43			
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	ID.GV-1	Se establece y se comunica la política de seguridad cibernética organizacional.	APO01.02		44			45,5
				APO13.01		47			
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	ID.GV-4	Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	EDM03.02		48			42,5
				DSS04.02		37			
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	ID.RA-1	Se identifican y se documentan las vulnerabilidades de los activos.	APO12.01		42			40,5
				APO12.03		39			
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	ID.RA-5	Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	APO12.02		44			44
1. IDENTIFICAR (ID)	5. Estrategia de gestión de riesgos (ID.RM)	ID.RM-1	Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	APO13.02		43			43
				BAI02.03		43			

Perfil Actual Función Proteger

Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	Nivel Implementación				Promedio
					N	P	L	F	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1	Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	DSS05.04		49			45,5
				DSS06.03		42			
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-2	Se gestiona y se protege el acceso físico a los activos.	DSS01.04		49			45,5
				DSS06.03		42			
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-3	Se gestiona el acceso remoto.	BAI09.02			60		60
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-5	Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	DSS05.02		41			41
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-6	Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	DSS05.07		42			42
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de	PR.AC-7	Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor	DSS05.04		49			49
2. PROTEGER (PR)	2. Concienciación y capacitación (PR.AT)	PR.AT-1	Todos los usuarios están informados y capacitados.	APO07.03		48			48
2. PROTEGER (PR)	2. Concienciación y capacitación (PR.AT)	PR.AT-2	Los usuarios privilegiados comprenden sus roles y responsabilidades.	APO07.02		40			40
2. PROTEGER (PR)	2. Concienciación y capacitación (PR.AT)	PR.AT-5	El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	DSS06.03		42			42
2. PROTEGER (PR)	3. Seguridad de los datos (PR.DS)	PR.DS-1	Los datos en reposo están protegidos.	APO14.04		43			43
2. PROTEGER (PR)	3. Seguridad de los datos (PR.DS)	PR.DS-2	Los datos en tránsito están protegidos.	APO14.05		42			42
2. PROTEGER (PR)	4. Procesos y procedimientos de protección de la información	PR.IP-4	Se realizan, se mantienen y se prueban copias de seguridad de la información.	APO13.01		47			47
2. PROTEGER (PR)	5. Mantenimiento (PR.MA)	PR.MA-2	El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	DSS05.04		49			49
2. PROTEGER (PR)	6. Tecnología de protección (PR.PT)	PR.PT-4	Las redes de comunicaciones y control están protegidas.	APO13.01		47			47
2. PROTEGER (PR)	6. Tecnología de protección (PR.PT)	PR.PT-5	Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.	BAI04.01			50		50

Perfil Actual Función Detectar

Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	Nivel Implementación				Promedio
					N	P	L	F	
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-1	Se monitorea la red para detectar posibles eventos de seguridad cibernética.	DSS03.05		43			43
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-2	Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	DSS01.04		49			49
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-4	Se detecta el código malicioso.	DSS05.01		47			47
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-7	Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	DSS05.02		41			41
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-8	Se realizan escaneos de vulnerabilidades.	DSS05.07		42			42
3. DETECTAR (DE)	3. Procesos de Detección (DE.DP)	DE.DP-2	Las actividades de detección cumplen con todos los requisitos aplicables.	DSS06.03		42			42

Perfil Actual Función Responder

Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	Nivel Implementación				
					N	P	L	F	Promedio
4. RESPONDER (RS)	1. Planificación de la Respuesta (RS.RP)	RS.RP-1	El plan de respuesta se ejecuta durante o después de un incidente.	APO12.06		45			45
4. RESPONDER (RS)	2. Comunicaciones (RS.CO)	RS.CO-1	El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	EDM03.02		48			48
4. RESPONDER (RS)	2. Comunicaciones (RS.CO)	RS.CO-3	La información se comparte de acuerdo con los planes de respuesta.	DSS03.03		41			41
4. RESPONDER (RS)	2. Comunicaciones (RS.CO)	RS.CO-4	La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	DSS03.04		47			47
4. RESPONDER (RS)	3. Análisis (RS.AN)	RS.AN-1	Se investigan las notificaciones de los sistemas de detección.	DSS02.04		43			43
4. RESPONDER (RS)	4. Mitigación (RS.MI)	RS.MI-1	Los incidentes son contenidos.	DSS05.03		47			47
4. RESPONDER (RS)	4. Mitigación (RS.MI)	RS.MI-2	Los incidentes son mitigados.	DSS05.07		42			42

Perfil Actual Función Recuperar

Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	Nivel Implementación				
					N	P	L	F	Promedio
5. RECUPERAR (RC)	1. Planificación de la recuperación (RC.RP)	RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	APO12.06		45			45

Criterios Quick wins

- Se seleccionan las prácticas de COBIT 2019 que estén alineadas a los objetivos de gobierno y gestión determinadas en el Paso 1 Alcance del modelo alineado a los objetivos empresariales. Además de las actividades de los objetivos de gobierno y gestión que permitan mitigar el nivel de impacto de los riesgos considerados como inaceptables y moderados.

- La probabilidad de éxito y el Impacto positivo en el negocio. La escala que se utilizará será Alto, Medio y Bajo, cada una con un valor de 3,2,1 respectivamente. El nivel de prioridad será el resultado de multiplicar los valores asignados de probabilidad e impacto y se seleccionaran los que tenga los valores más altos.

Quick wins

Subcategoría CSF	Práctica Cobit 2019	PE	IPN	Prioridad
ID.GV-4, RS.CO-1	EDM03.02 Act.4	2	3	6
ID.GV-4, RS.CO-1	EDM03.02 Act.5	2	3	6
ID-RA-1	APO12.01 Act.3	2	3	6
ID-RA-1	APO12.01 Act.7	2	3	6
ID-RA-5	APO12.02 Act.1	2	3	6
ID-RA-5	APO12.02 Act.3	2	3	6
ID-RA-5	APO12.02 Act.7	3	2	6
ID-RA-5	APO12.02 Act.8	2	3	6
ID-RA-1	APO12.03 Act.1	2	3	6
ID-RA-1	APO12.03 Act.2	2	3	6
RS.RP-1	APO12.06 Act.1	2	3	6
RS.RP-1	APO12.06 Act.2	3	2	6
ID.RM-1	BAI02.03 Act.3	2	3	6
ID.AM-2	BAI09.05 Act.1	3	2	6
ID.AM-2	BAI09.05 Act.3	3	2	6
ID.GV-4	DSS04.02 Act.2	2	3	6
ID.GV-4	DSS04.02 Act.5	3	2	6
ID.GV-4	DSS04.02 Act.6	3	2	6
ID.GV-4	DSS04.02 Act.7	3	2	6
DE.CM-4	DSS05.01 Act.3	2	3	6
PR.AC-5, DE.CM-7	DSS05.02 Act.1	2	3	6
PR.AC-5, DE.CM-7	DSS05.02 Act.4	2	3	6

Subcategoría CSF	Practica Cobit 2019	PE	IPN	Prioridad
PR.AC-5, DE.CM-7	DSS05.02 Act.5	3	2	6
PR.AC-5, DE.CM-7	DSS05.02 Act.7	2	3	6
PR.AC-5, DE.CM-7	DSS05.02 Act.8	3	3	9
RS.MI-1	DSS05.03 Act.5	2	3	6
RS.MI-1	DSS05.03 Act.9	2	3	6
PR.AC-1, PR.AC-7,PR.MA-2	DSS05.04 Act.5	2	3	6
PR.AC-1, PR.AC-7,PR.MA-2	DSS05.04 Act.6	2	3	6
PR.AC-1, PR.AC-7,PR.MA-2	DSS05.04 Act.8	3	3	9
PR.AC-6, DE.CM-8	DSS05.07 Act.3	2	3	6
PR.AC-1, PR.AT-5, DE.DP-2	DSS06.03 Act.1	2	3	6
PR.AC-1, PR.AT-5, DE.DP-2	DSS06.03 Act.4	3	3	9
PR.AC-1, PR.AT-5, DE.DP-2	DSS06.03 Act.6	2	3	6

Modelo Función Identificar

Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Brechas: Práctica	Brechas: Subcategoría	Solución de Ciberseguridad	Indicadores	Responsables
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	ID.AM-2	BAI09.05	47	L	Act.1		Herramientas de Gobernanza, Riesgo y Cumplimiento GRC	% licencias usadas vs compradas, % de licencias y productos que deben actualizarse	Gerencia Nacional Técnica, Jefatura de O&M Transmisión
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	ID.GV-4	EDM03.02	42.5	L	Act.4, Act.5		Gestor de Seguridad de la Información y Eventos	% de proyectos que consideran el riesgo cibernético, nivel de alineamiento entre el riesgo empresarial y el cibernético	
			DSS04.02			Act.2, Act.5, Act 7			% de stakeholders involucrados en evaluaciones de impacto del negocio	
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	ID.RA-1	APO12.01	40.5	L	Act.1, Act.3		Gestor de Seguridad de Infraestructura de Red	Número de eventos con pérdidas y características principales	
			APO12.03			Act.1, Act.2			% de procesos principales del negocio en el perfil de riesgo	
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	ID.RA-5	APO12.02	44	L	Act.1, Act.3, Act.7, Act.8			Número de escenarios identificados de riesgos	
1. IDENTIFICAR (ID)	5. Estrategia de gestión de riesgos (ID.RM)	ID.RM-1	BAI02.03	43	L	Act.3			% de requerimientos de riesgo no cubiertos por una acción de respuesta	

Modelo Función Proteger

					Brechas					
Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Práctica	Subcategor	Solución de Ciberseguridad	Indicadores	Responsables
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1	DSS05.04	45.5	L	Act.5, Act.6,Act.8		Next Generation Firewall	Promedio de tiempo entre cambio y actualización de cuentas	Jefatura de O&M Transmisión
			DSS06.03			Act.1, Act.4,Act.6			% de roles con derechos de acceso y niveles de autoridad	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-2	DSS06.03	45.5	L	Act.1, Act.4,Act.6		Encripción de Discos	Número de incidentes por violación a los permisos de ingreso	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-5	DSS05.02	41	L	Act.1, Act.4, Act.5, Act.7		Control de Acceso de Red NAC	Número de brechas en el firewall	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-6	DSS05.07	42	L	Act.3		Control de Acceso de Usuarios Privilegiados	Número de cuentas vs Número de usuarios autorizados	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-7	DSS05.04	49	L	Act.5, Act.6,Act.8			Número de incidentes relacionados a acceso no autorizado a la información	
2. PROTEGER (PR)	2. Concienciación y capacitación (PR.AT)	PR.AT-5	DSS06.03	42	L	Act.1, Act.4,Act.6		Encripción de datos basados en Roles	% de roles con clara separación de rutinas	
2. PROTEGER (PR)	5. Mantenimiento (PR.MA)	PR.MA-2	DSS05.04	49	L	Act.5, Act.6,Act.8		Aplication Delivery Controller	% de equipos actualizados a las últimas versiones	

Modelo Función Detectar

						Brechas				
Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Práctica	Subcategor	Solución de Ciberseguridad	Indicadores	Responsables
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-4	DSS05.01	47	L	Act.3		NGFW	Número de ataques de software maliciosos exitosos	Jefatura de O&M Transmisión
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-7	DSS05.02	41	L	Act.1, Act.4, Act.5, Act.7		IPS /IDS	% de tiempo de conexión inusual a los sistemas	
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-8	DSS05.07	42	L	Act.3		Endpoint Detección de amenazas	Número de pruebas de vulnerabilidad realizadas a los equipos perimetrales	
3. DETECTAR (DE)	3. Procesos de Detección (DE.DP)	DE.DP-2	DSS06.03	42	L	Act.1, Act.4,Act.6		Analisis de comportamiento de Red	% de actividades que cumplen con los requisitos propuestos	

Modelo Función Responder

						Brechas				
Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Práctica	Subcategoría	Solución de Ciberseguridad	Indicadores	Responsables
4. RESPONDER (RS)	1. Planificación de la Respuesta (RS.RP)	RS.RP-1	APO12.06	45	L	Act.1, Act.2			% de acciones ejecutadas vs las diseñadas en el plan de respuesta	Jefatura de O&M Transmisión
4. RESPONDER (RS)	2. Comunicaciones (RS.CO)	RS.CO-1	EDM03.02	48	L	EDM03.02 Act.4, Act 5		Endpoint Detección de amenazasy respuesta ETDR	% del personal que tiene conocimiento de sus funciones	
4. RESPONDER (RS)	4. Mitigación (RS.MI)	RS.MI-1	DSS05.03	47	L	Act.5, Act.9		Automatización de SOC	Número de Incidentes contenidos	
4. RESPONDER (RS)	4. Mitigación (RS.MI)	RS.MI-2	DSS05.07	42	L	Act.3		Herramientas de Inteligencia de Amenazas	Número de Incidentes mitigados	

Modelo Función Recuperar

					Brechas					
Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Práctica	Subcategoría	Solución de Ciberseguridad	Indicadores	Responsables
5. RECUPERAR (RC)	1. Planificación de la recuperación (RC.RP)	RC.RP-1	APO12.06	45	L	Act.1, Act.2		Herramientas de DR y COOP	% de recuperación de operaciones del giro del negocio	Jefatura de O&M Transmisión

Conclusiones

- La caracterización y valoración de los componentes de la red de transmisiones de la CNT determinó que la mayor parte de los activos con que se operan son críticos para el giro de negocio. De esta manera se logró establecer al área de Transmisiones como el núcleo de operaciones de la CNT y por lo tanto es una infraestructura critica para el país.

- Se realizó un análisis de riesgo basado en la metodología NIST 800-30, enfocado en identificar las fuentes de amenaza, eventos de amenaza y vulnerabilidades. En base a su frecuencia de ocurrencia y su nivel de impacto se determinó que seis riesgos son inaceptables, diecisiete son moderados y seis son aceptables Este análisis es la base para el diseño del modelo de ciberseguridad al identificar las brechas en los perfiles de ciberseguridad del marco de la NIST.

Conclusiones

- Los factores de diseño y la cascada de metas de COBIT 2019 son elementos claves para determinar los seis objetivos de gobierno y gestión específicos alineados a la estrategia empresarial de esta infraestructura critica . Por lo tanto, COBIT 2019 se alinea a los requerimientos de la alta dirección de la CNT para optimizar el riesgo cibernético

- El marco de ciberseguridad para infraestructuras críticas de la NIST está compuesto por funciones, categorías y subcategorías, las cuales alineadas a las prácticas de COBIT 2019 determinaron que el nivel actual de ciberseguridad de la CNT es de Tier 2 Riesgo Informado y el nivel deseado en todas las prácticas de COBIT 2019 correspondientes a las subcategorías del marco es Largamente Ejecutado.

Conclusiones

- Los criterios para el análisis, priorización de brechas y oportunidades tales como la probabilidad de éxito y el impacto positivo de negocio, definieron veinte y uno proyectos quick wins los cuales optimizarán los procesos con una inversión baja mejorando así el nivel de ciberseguridad de la empresa.

- El diseño del modelo de ciberseguridad alineado a COBIT y al CSF estableció que es necesario diecisiete soluciones de ciberseguridad, veinte y cuatro indicadores y una gerencia responsable. Por lo tanto, el modelo propuesto es la base para que las actividades de gobierno y gestión de la empresa generen valor a través de la optimización del riesgo cibernético con un enfoque de mejora continua.

Recomendaciones

- Planificar y ejecutar capacitaciones a todos los servidores del área de Transmisiones para la socialización de temas de marcos de trabajos para gobierno y gestión las tecnologías de información y de ciberseguridad en infraestructura críticas, con el propósito de implementar adecuadamente el modelo propuesto y dar inicio a la cultura corporativa empresarial con enfoque en ciberseguridad.

- Implementar las soluciones de ciberseguridad correspondientes a cada función del CSF , realizar un monitoreo continuo del rendimiento y un informe con los indicadores establecidos para justificar a la alta gerencia la inversión realizada en términos de amenazas y riesgos mitigados.

Recomendaciones

- Revisar el nivel de implementación de todas las categorías del marco de ciberseguridad periódicamente para determinar si están dando soporte a conseguir los objetivos empresariales o se necesita algún tipo de corrección en los procesos de las prácticas de COBIT 2019.

- Para mantener la disponibilidad de los servicios de manera interna y externamente a la empresa, se debe realizar un plan de mantenimiento preventivo y correctivo a todos los activos que están bajo la responsabilidad del área de Transmisiones de la CNT para la correcta gestión a nivel físico y lógico.

dariotipan1952@hotmail.com