Ciberseguridad Sector Eléctrico

Acuerdo 1502 – Guía Ciberseguridad

Comité de Ciberseguridad

Consejo Nacional de Operación

Colombia inteligente

Juan D. Molina

01 de febrero, 2024

NOTA DE RESPONSABILIDAD –

Las opiniones que contenga este documento son parte de un ejercicio en desarrollo de identificación y análisis sectorial para consolidar acciones de transformación del sector eléctrico colombiano y no necesariamente representan la opinión oficial de una organización, entidad o empresa.

La veracidad de los datos recopilados y utilizados en el presente documento no es puesta en duda por parte de Colombia Inteligente, no haciéndose responsable por su exactitud ni su integridad.

Antecedentes

Acuerdo 788
Guía de Ciberseguridad del sector eléctrico

Referente NERC-CIP
002 - 009

1. Ciberseguridad
2. Identificación de activos críticos
3. Gestión de la seguridad de ciber activos críticos
4. Seguridad física de ciber activos críticos
5. Plan de recuperación de ciber activos críticos

Anexo 1 – Criterio de activos críticos (15)

Acuerdo 1241
Cir. CNO 34

Referente NERC-CIP
002 - 014

1. Ciberseguridad
2. Aplicación
3. Cumplimiento
4. Identificación de activos críticos
5. Gobierno y gestión del personal
6. Perímetro
7. Gestión de la seguridad de ciberactivos críticos
8. Plan de recuperación de ciberactivos críticos
9. Plan de respuesta ante incidentes en ciberactivos críticos
10. Seguridad física de ciberactivos críticos

Anexo 1 – Criterio de activos críticos (9)
Anexo 2 – Lista de cumplimiento periódico de la guía de ciberseguridad
Agradecimientos

Acuerdo 1347

- Monitoreo
- Implementación Guía (semestral)
- Ampliación tiempos (COVID-19)

Acuerdo 1463/1502
Revisión 2021

- Ampliación tiempos (COVID-19)

Referente NERC-CIP
002 - 014

1. Ciberseguridad
2. Aplicación
3. Cumplimiento
4. Identificación de activos críticos
5. Gobierno y gestión del personal
6. Perímetro
7. Gestión de la seguridad de ciberactivos críticos
8. Plan de recuperación de ciberactivos críticos
9. Plan de respuesta ante incidentes en ciberactivos críticos
10. Seguridad física de ciberactivos críticos
11. Gestión de la cadena de suministro

Anexo 1 – Criterio de activos críticos (9)
Anexo 2 – Lista de cumplimiento periódico de la guía de ciberseguridad
Agradecimientos

Persona responsable de dirigir y administrar la implementación de la Guía de Ciberseguridad (Marzo 3 de 2016)

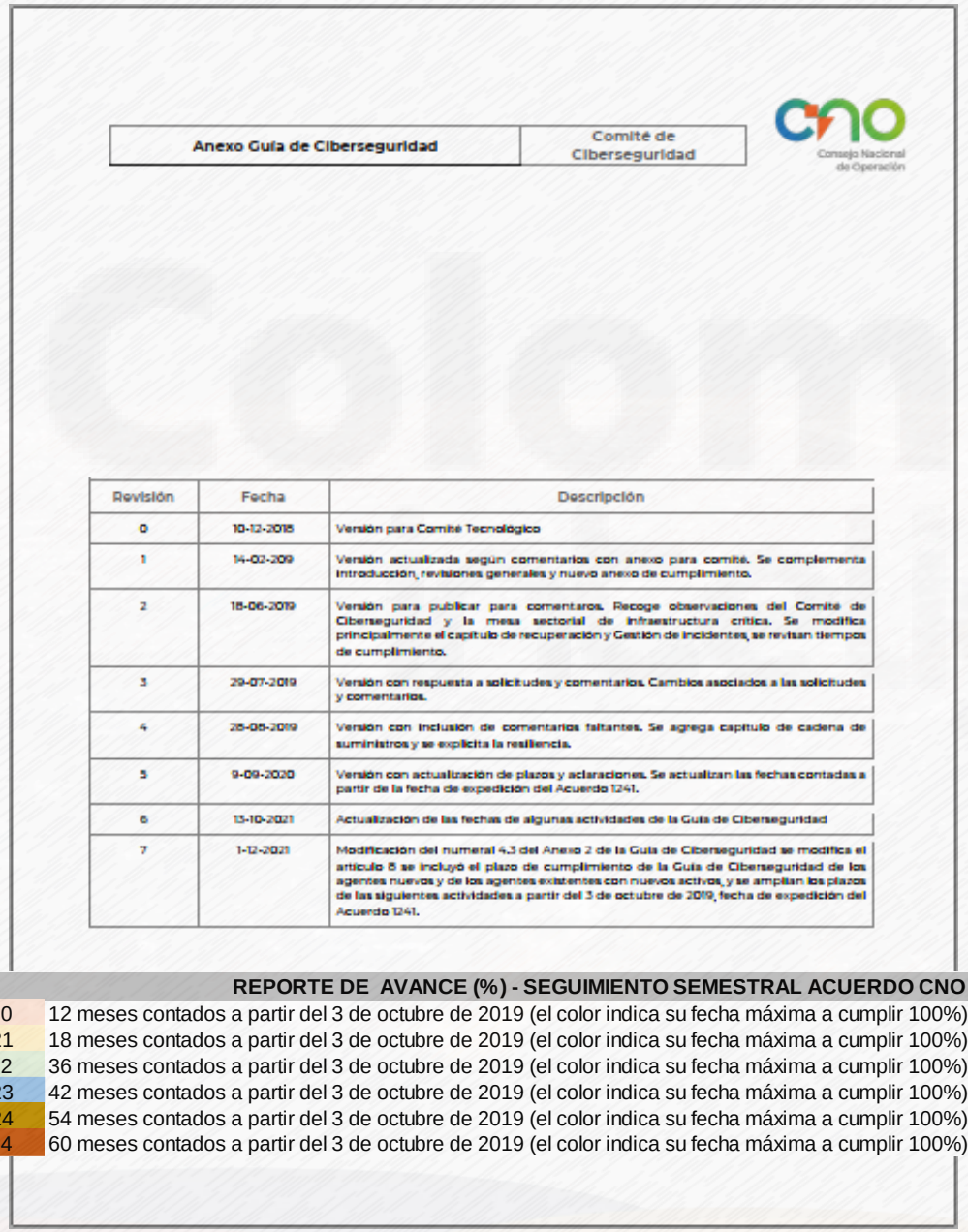
Comisión temporal ciberseguridad

2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022

Acuerdo 701
Seguridad e integridad lecturas

Acuerdo 1004/1043
Actualización seguridad e integridad lecturas

Acuerdo 1502



Anexo Guía de Ciberseguridad	Comité de Ciberseguridad

Consejo Nacional de Operación

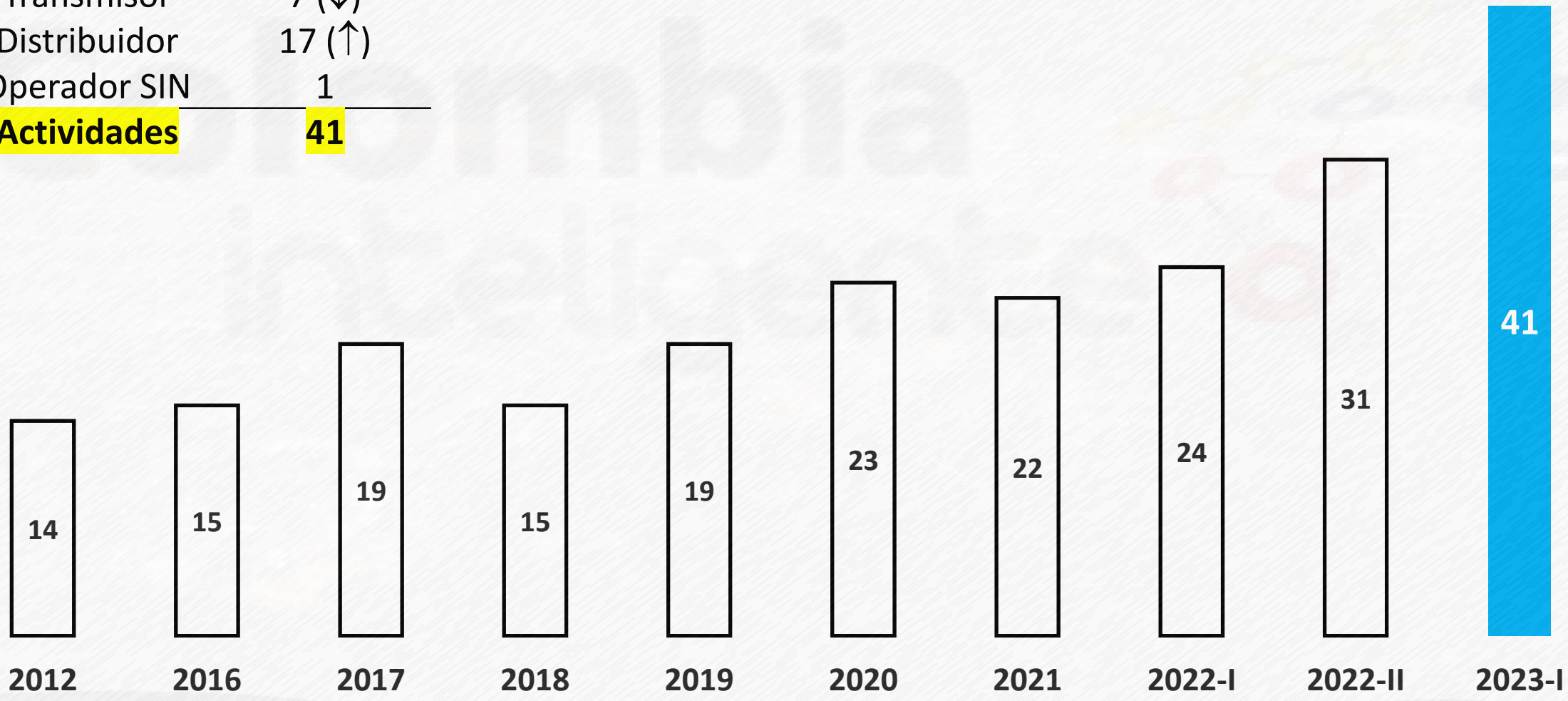
Revisión	Fecha	Descripción
0	10-12-2018	Versión para Comité Tecnológico
1	14-02-2019	Versión actualizada según comentarios con anexo para comité. Se complementa introducción, revisiones generales y nuevo anexo de cumplimiento.
2	18-06-2019	Versión para publicar para comentarios. Recoge observaciones del Comité de Ciberseguridad y la mesa sectorial de infraestructura crítica. Se modifica principalmente el capítulo de recuperación y Gestión de incidentes, se revisan tiempos de cumplimiento.
3	29-07-2019	Versión con respuesta a solicitudes y comentarios. Cambios asociados a las solicitudes y comentarios.
4	28-08-2019	Versión con inclusión de comentarios faltantes. Se agrega capítulo de cadena de suministros y se explicita la resiliencia.
5	9-09-2020	Versión con actualización de plazos y aclaraciones. Se actualizan las fechas contadas a partir de la fecha de expedición del Acuerdo 1241.
6	13-10-2021	Actualización de las fechas de algunas actividades de la Guía de Ciberseguridad
7	1-12-2021	Modificación del numeral 4.3 del Anexo 2 de la Guía de Ciberseguridad se modifica el artículo 8 se incluyó el plazo de cumplimiento de la Guía de Ciberseguridad de los agentes nuevos y de los agentes existentes con nuevos activos, y se amplían los plazos de las siguientes actividades a partir del 3 de octubre de 2019, fecha de expedición del Acuerdo 1241.

REPORTE DE AVANCE (%) - SEGUIMIENTO SEMESTRAL ACUERDO CNO 1502	
oct-20	12 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).
abr-21	18 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).
oct-22	36 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).
abr-23	42 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).
abr-24	54 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).
oct-24	60 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).

5.3.2	Marque (x)	¿Se encuentra actualizado ante el CNO el responsable de ciberseguridad que debe ser reportado antes del 3 de abril de 2020?	
		SI	
		NO	
Política o lineamiento de ciberseguridad			
5.3.1	%	Política y lineamiento de ciberseguridad	
Plan de sensibilización y entrenamiento para el personal relacionado con ciberactivos			
5.3.4	%	Programa de conciencia de seguridad	
5.3.5	%	Programa de entrenamiento y capacitación	
Plan de gestión de incidentes de ciberseguridad			
9.3.1	%	Plan de respuesta ante incidentes	
9.3.2	%	Documentación de pruebas o simulacros	
9.3.3	%	Registro de cambios del procedimiento respuesta a incidentes	
Actualización de inventario de ciberactivos			
4.3.1	%	Activos críticos	
4.3.2	%	Ciberactivos críticos	
Seguridad electrónica de ciberactivos			
6.3.1	%	Perímetros de seguridad electrónica	
5.3.6	%	Administración de accesos	
5.3.7	%	Verificación de los registros de autorización	
5.3.8	%	Verificación de cuentas y privilegios de acceso	
5.3.9	%	Procedimiento de revocación de accesos	
7.3.1	%	Procedimiento de control de cambios y gestión de configuraciones	
7.3.2	%	Herramientas de prevención de malware	
7.3.3	%	Procedimiento de evaluación de vulnerabilidades	
7.3.4	%	Procedimiento de control ciberactivos críticos transitorios y medios extraíbles	
7.3.5	%	Procedimiento de actualizaciones y parches de seguridad	
Seguridad física para ciberactivos			
10.3.1	%	Plan de seguridad física	
10.3.3	%	Procedimiento de control de visitantes	
10.3.4	%	Procedimiento de mantenimiento y pruebas	
Recuperación para ciberactivos			
8.3.1	%	Plan de recuperación y resiliencia	
8.3.2	%	Plan de pruebas o simulacros	
8.3.3	%	Registro de cambios del procedimiento de recuperación y resiliencia	
8.3.4	%	Respaldos y almacenamiento de información	
8.3.5	%	Registro de pruebas a los respaldos y mecanismos de contingencia y continuidad	
Primera ejecución del plan de sensibilización y entrenamiento para el personal relacionado con ciberactivos			
5.3.4	%	Programa de conciencia de seguridad	
5.3.5	%	Programa de entrenamiento y capacitación	
Implementación de los controles en los perímetros de seguridad electrónicos y físicos en acuerdo a los planes desarrollados			
6.3.1	%	Perímetros de seguridad electrónica	
6.3.2	%	Listas de acceso	
6.3.4	%	Validación de cambios	
6.3.5	%	Procedimiento para habilitar los puntos de acceso	
6.3.6	%	Procedimiento para la administración de conexiones temporales	
6.3.7	%	Sistema de control intermedio	
10.3.2	%	Restricción de acceso físico	
Implementación de monitoreo básico de eventos sobre los ciberactivos críticos			
6.3.3	%	Procedimiento de monitoreo y registro de acceso	
7.3.6	%	Procedimiento para identificar y monitorear eventos	
Gestión y evaluación ciberseguridad			
11.3.1	%	Plan de gestión de riesgo de la cadena de suministro (actualizado máximo a 24 meses)	
5.3.3	%	Evaluación personal y riesgos	
-	%	Actualización del nivel de gestión de ciberseguridad (análisis de brecha frente a la guía)	
-	%	Actualización del análisis de riesgos y vulnerabilidades	
Soporte cumplimiento			
3	%	Documentación (revisar, actualizar y conservar información soporte 3 años)	
-	%	Desarrollo primera auditoría interna (entre el mes de **octubre de 2021** y el mes de **abril del 2022**).	
Avance Implementación Guía de Ciberseguridad - Ciberactivos críticos			
a	%	Para el 50% de sus ciberactivos críticos - (42) cuarenta y dos meses contados a partir del 3 de octubre de 2019.	
b	%	Para el 75% de sus ciberactivos críticos - (54) cuarenta y dos meses contados a partir del 3 de octubre de 2019.	
c	%	Para el 100% de sus ciberactivos críticos - (60) cuarenta y dos meses contados a partir del 3 de octubre de 2019.	

Seguimiento entrega reporte

Agente	2023-I
Generador	16 (↓)
Transmisor	7 (↓)
Distribuidor	17 (↑)
Operador SIN	1
Actividades	**41**



Cobertura reporte

Acuerdo	1502	Activos	Fuente
Generación	≥ 20 MW	18.125 MW (68 Plantas) Total SIN: 19.888 (276 Recursos)	Capacidad Generación XM – Paratec
Recursos potencia reactiva (excepto generadores)	NIV - STN	OR/TN/TR	Agente
Subestaciones NIV - STN (transformación)	NIV - STN	76.539 MVA 50# / ≥110 kV	Cap. Transformación XM – Paratec STR-NIV OR Creg 015/2018
FACTS	NIV - STN	7	ISA-ITCO-TSCA/GEB-ENLAZA/EPM
Esquemas de protección	Esquemas suplementarios (confiabilidad)	-	Agente
Sist. EDAC (v, f)	Todos	-OR-	Agente
Centro de control -ppal/respaldo-	G/T/D/Operador	G/T/D-OR/OS 22/14/39/1	Registro Agentes
Activos interconexiones internacionales	Todos	≈ 4 ctos (Ecuador) / 2 TN	CREG 187/2020
Activos (operación confiable SIN)	Entidad responsable que estime adecuado incluir	-	Agente

¿Cobertura reporte? – Información indicativa

Agentes

Actividad	#
Comercialización	132
Generación	108
Distribución	39
Transporte	14
Registrados	**293**

Actividad	A.1502
Distribución	39
Generación	22
Transporte	14
Operador	1
Alcance	**76**

Fuente: XM (abr, 2023)
http://paratec.xm.com.co/paratec/SitePages/Default.aspx
https://sinergox.xm.com.co/

Plantas

Agente	Cap. MW	# Plantas
ACPM	936	5
AGUA	13.206	158
BAGAZO	200	13
BIOGAS	11	5
CARBON	1.664	17
COMBUSTOLEO	268	4
GAS	3.104	29
JET-A1	50	1
RAD SOLAR	476	312
VIENTO	*18*	*1*
Total	**19.911**	**543**

Capacidad efectiva ≥ 20 MW

+22 Agentes

Agente	Cap. MW	# Plantas
ACPM	900	3
AGUA	12.237	30
BAGAZO	60	1
CARBON	1.634	14
COMBUSTOLEO	266	4
GAS	2.975	15
JET-A1	50	1
Total	**18.125**	**68**

CHVG, EMUG, ENDG, EPMG, EPSG, GECG, HDPG, HIMG, ISGG, NTCG, PRIG, SFEG, SOCG, TBSG, TCIG, TEMG, TERG, TMFG, TMNG, TMVG, TRMG, TYPG, …

Redes/Transformación

Nivel	Redes		Transformación	
kV	km	Agentes	MVA	Agentes
110	3.899	12	10.585	14
115	8.398	21	12.587	38
116,8	-	-	51	1
123,54	-	-	216	1
138	15	1	40	1
220	2.598	4	14.279	16
230	10.959	9	22.505	20
500	3.655	2	16.278	5
Total	**29.347**		**76.540**	

Nivel 4 (≥ 57,5 kV y menor a 220 kV) + STN

+50 Agentes

OPERADOR DE RED (29): CASD, CDID, CDND, CEOD, CETD, CHCD, CMMD, CNSD, CQTD, CSSD, CTID, EBPD, EBSD, EDPD, EDQD, EEPD, EGVD, EMED, EMID, EMSD, ENDD, ENID, EPMD, EPSD, EPTD, ESSD, EVSD, HLAD, RTQD.

TRANSMISOR NACIONAL (14): CHCT, CNST, DEST, DIST, EBST, EEBT, EPMT, EPST, ESST, ISAT, ITCT, SAPT, TCET, TRST.

TRANSMISOR REGIONAL (7): CNAD, CNGD, EEAD, EEBD, EERD, NORD, TECD.

Cobertura reporte

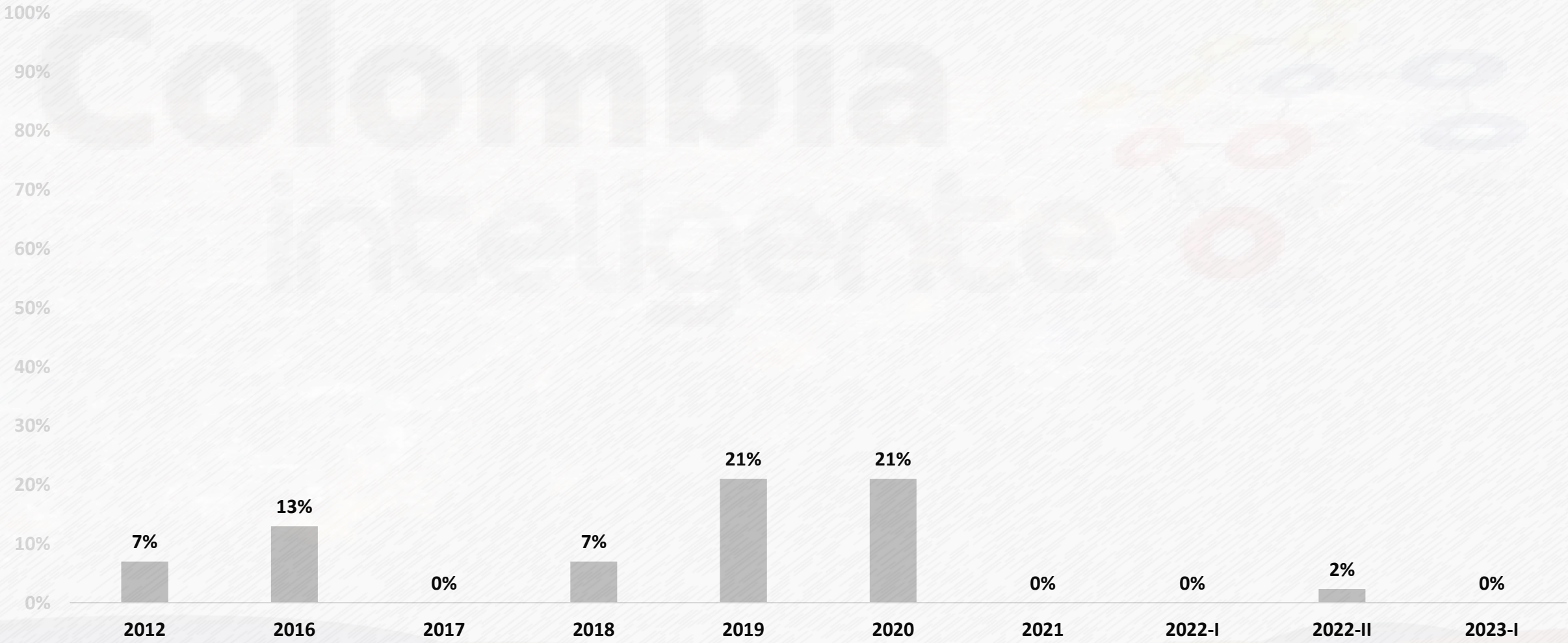
Acuerdo	Activos	Reporte 2022-II (*)	Reporte 2023-I (*)
Generación ≥ 20 MW	18.125 MW (68 Plantas)	14.145,9 (155 Plantas)	13.169 (67 Plantas) ↓
Recursos potencia reactiva (excepto generadores) NIV - STN	OR/TN/TR	1.529,2 MVaR	1.760 MVaR (68) ↑
Subestaciones NIV - STN (transformación)	76.539 MVA 50# / ≥110 kV	21.293,501 MVA	24.002 MVA (581) ↑
FACTS NIV - STN	7	7	23 ↑
Esquemas de protección	-	66	749 ↑
Sist. EDAC (v, f)	-OR-	635	809 ↑
Centro de control -ppal/respaldo- (Empresas)	G/T/D-OR/OS 22/14/39/1	14/6/10/1 63,6%/37,5%/33,3%/100% 39	14/6/10/1 63,6%/37,5%/33,3%/100% 52 ↑
Activos interconexiones internacionales	4 ctos (Ecuador) 2 TN	5	9 ↑
Activos (operación confiable SIN)	-	227 AGC, Servidores de aplicaciones, dispositivos perimetrales, dispositivos de comunicación.	339 ↑

(*) Reporte realizado por cada agente en el diligenciamiento del reporte Acuerdo CNO 1502.

Avances

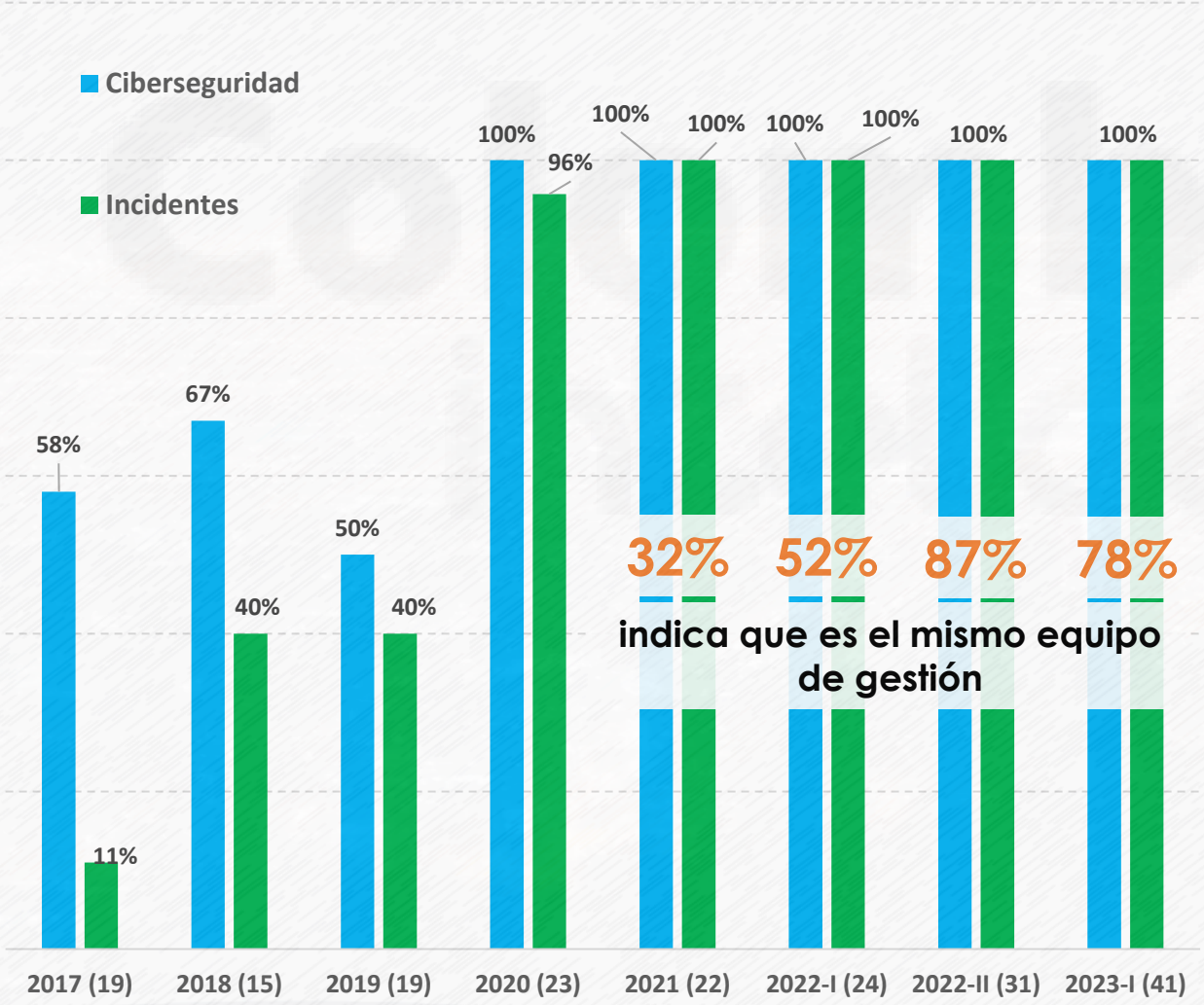
Gestión sectorial: incidentes

¿Se han presentado incidentes de ciberseguridad o eventos no explicados sobre los activos críticos?



Avances

Gestión sectorial: equipo de ciberseguridad



Equipo gestión de ciberseguridad

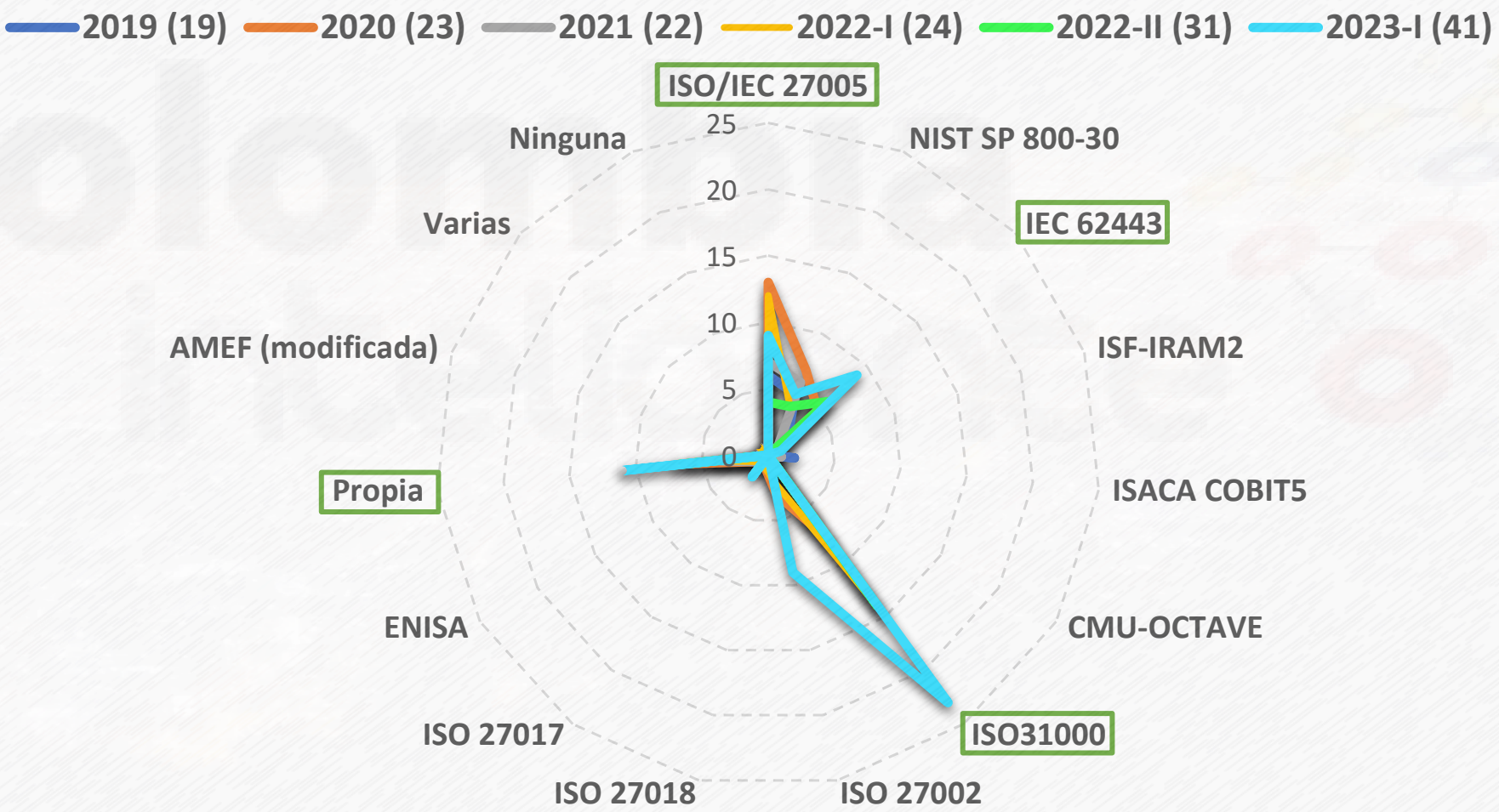
Rango (#)	2019 (19)	2020 (23)	2021 (24)	2022-I (31)	2022-II (43)	2023-I (41)
1	7,10%	8,7%	4,5%	9,7%	9,7%	4,9%
2-3	**35,70%**	**43,5%**	**45,5%**	**41,9%**	**38,7%**	31,7%
4-5	28,60%	21,7%	22,7%	16,1%	12,9%	**36,6%**
> 5	28,60%	26,1%	27,3%	32,3%	**38,7%**	26,8%

Equipo gestión incidentes de seguridad

Rango (#)	2019 (19)	2020 (23)	2021 (24)	2022-I (31)	2022-II (43)	2023-I (41)
1	20%	22,8%	0,0%	6,7%	9,7%	29,3%
2-3	**50%**	22,8%	33,3%	33,3%	**35,5%**	31,7%
4-5	0%	**27,2%**	**40,0%**	20,0%	19,4%	**34,1%**
> 5	30%	**27,2%**	26,7%	**40,0%**	**35,5%**	4,9%

Avances

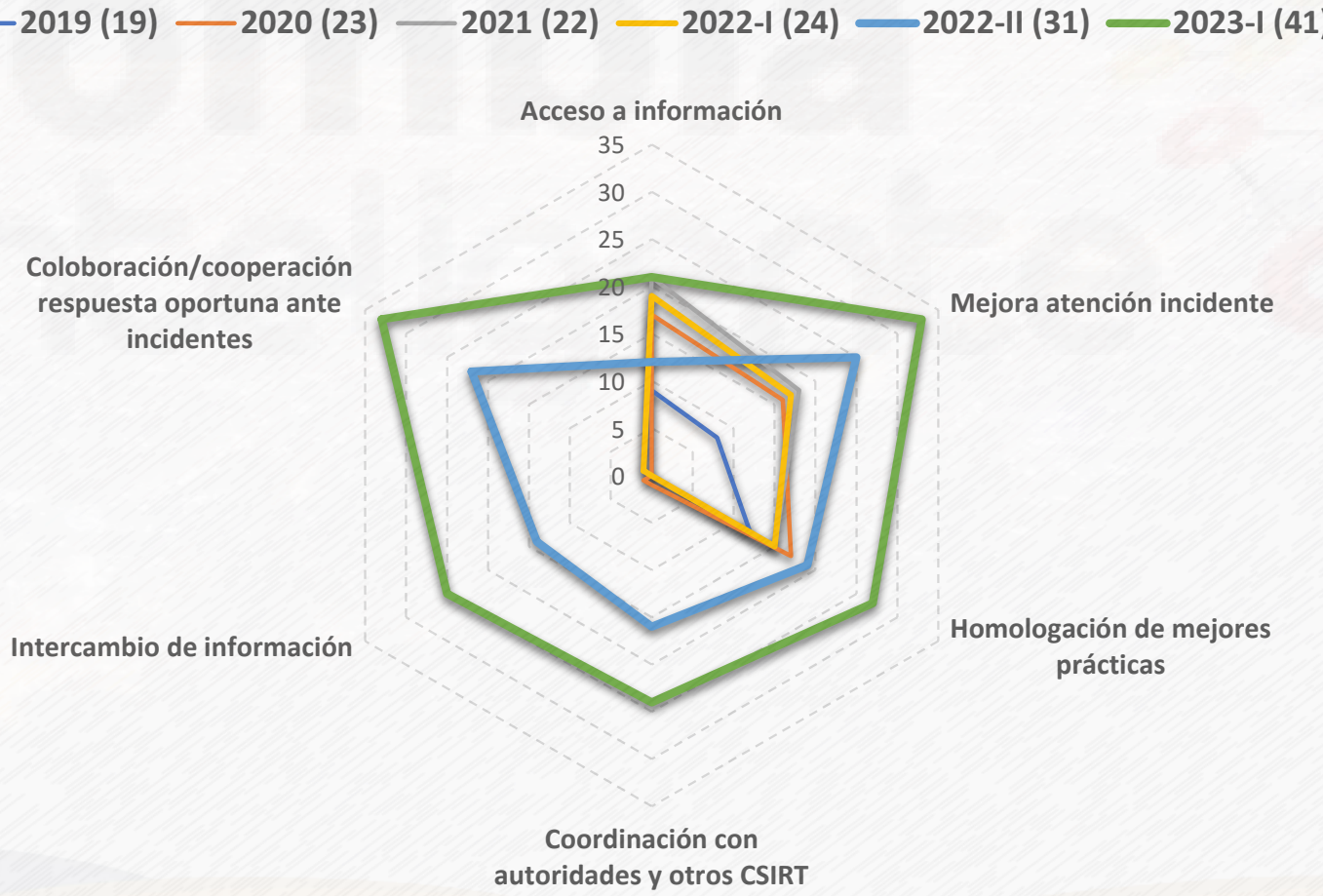
Gestión sectorial: metodología evaluación riesgos



Avances

Gestión sectorial: CSIRT

	2019 (19)	2020 (23)	2021 (22)	2022-I (31)	2022-II (43)	2023-I (41)
Conocimiento CSIRT	83,3%	95,7%	100%	97,2%	93,0%	**100%**



Beneficios de la implementación del CSIRT

MISP

97,5%

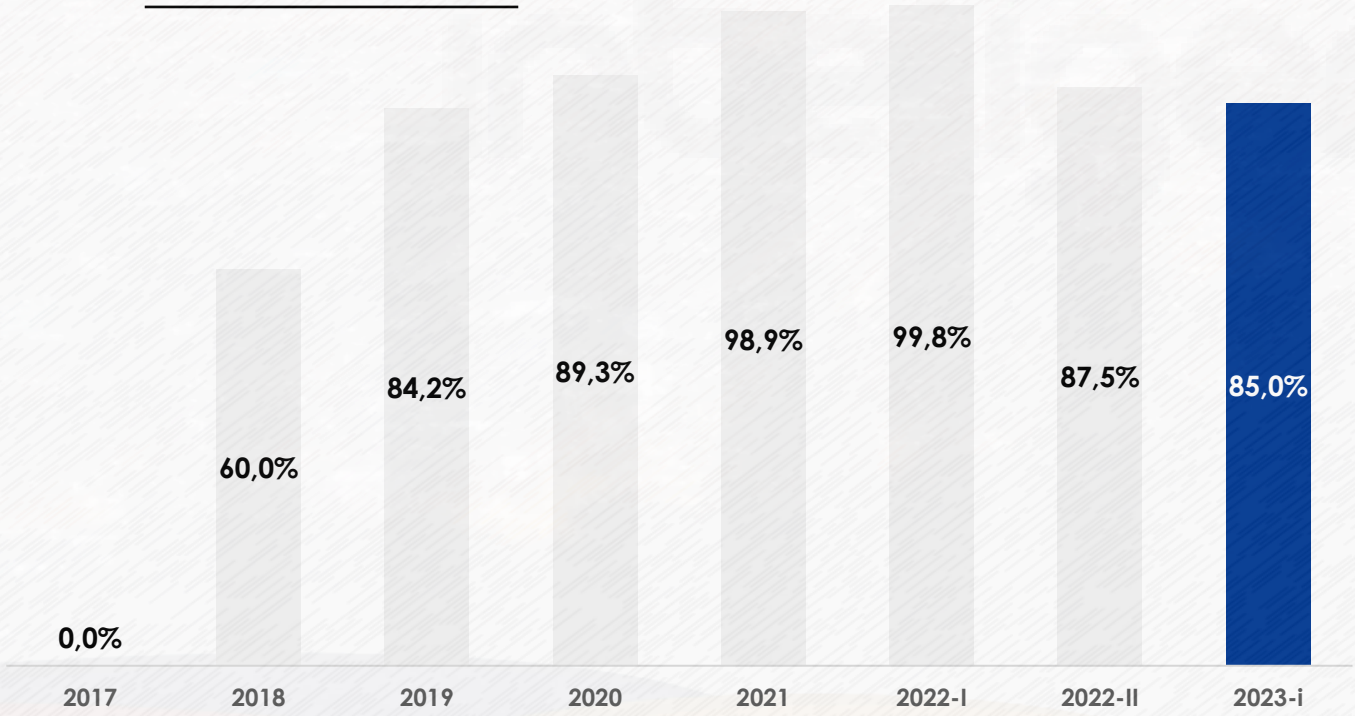
Indica que lo conoce

Avances

Gestión sectorial

Política o lineamiento de ciberseguridad – 5.3.1

Rango	#
0%	1
>0% - 25%	3
25% - 50%	3
50% - 75%	1
75% - 99%	5
100%	28



Responsable de ciberseguridad – 5.3.2

100%

Actualizado ante el CNO el responsable de ciberseguridad que debía ser reportado antes del 3 de abril de 2020

93,5%

Es importante lograr el seguimiento sobre el 100% de los Agentes (Actividades) establecidas en el Acuerdo CNO 1502.

+6 Generadores

+8 Transmisores

+19 Distribuidores

Mapa de Actividades
Acuerdo 1502
2023 Sem-I

REPORTE DE AVANCE (%) - SEGUIMIENTO SEMESTRAL ACUERDO CNO 1502		
oct-20	77,5%	12 meses contados a partir del 3 de octubre de 2019.
abr-21	93,5%	18 meses contados a partir del 3 de octubre de 2019.
abr-22	76,0%	Desarrollo primera auditoría interna (oct-2021 / abr-2022).
oct-22	74,1%	36 meses contados a partir del 3 de octubre de 2019.
abr-23	76,7%	Para el 50% de sus ciberactivos críticos (42m).
abr-24	65,7%	Para el 75% de sus ciberactivos críticos (54m).
oct-24	54,1%	Para el 100% de sus ciberactivos críticos (60m).

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

Num.	2023-I (41)	Actividad
5.3.1	85,0%	Política y lineamiento de ciberseguridad
5.3.2	93,5%	Responsable de ciberseguridad
5.3.5	82,7%	Programa de entrenamiento y capacitación
9.3.1	79,0%	Plan de respuesta ante incidentes
9.3.2	64,8%	Plan de pruebas o simulacros
4.3.1	95,4%	Activos críticos
4.3.2	92,0%	Ciberactivos críticos
-	74,8%	Análisis de riesgos
7.3.3	75,4%	Procedimiento de evaluación de vulnerabilidades
-	72,3%	Analisis de brecha frente a la guía
8.3.1	76,9%	Plan de recuperación
8.3.2	60,9%	Plan de pruebas o simulacros
6.3.1	83,1%	Perímetros de seguridad electrónica
5.3.4	87,6%	Programa de conciencia de seguridad
5.3.5	79,6%	Programa de entrenamiento y capacitación
5.3.9	77,4%	Procedimiento de revocación de accesos
7.3.1	70,0%	Procedimiento de control de cambios y gestión de configuraciones
7.3.4	69,7%	Procedimiento de control ciberactivos críticos transitorios y medios extraíbles
7.3.5	66,7%	Procedimiento de actualizaciones y parches de seguridad
11.3.1	62,1%	Plan de gestión de riesgo de la cadena de suministro
10.3.1	82,1%	Plan de seguridad física
5.3.3	73,0%	Evaluación personal y riesgos
10.3.3	85,5%	Procedimiento de control de visitantes
10.3.4	69,1%	Procedimiento de mantenimiento y pruebas
5.3.4	87,6%	Programa de conciencia de seguridad
5.3.5	79,6%	Programa de entrenamiento y capacitación
6.3.1	79,3%	Perímetros de seguridad electrónica
6.3.2	75,2%	Listas de acceso
6.3.4	67,7%	Validación de cambios
6.3.5	66,5%	Procedimiento para habilitar los puntos de acceso
6.3.6	68,8%	Procedimiento para la administración de conexiones temporales
6.3.7	62,7%	Sistema de control intermedio
10.3.2	79,2%	Restricción de acceso físico
6.3.3	69,1%	Procedimiento de monitoreo y registro de acceso
7.3.6	68,0%	Procedimiento para identificar y monitorear eventos
3	73,6%	Cumplimiento (revisar, actualizar y conservar información soporte, 3años)
5.3.6	80,7%	Administración de accesos
5.3.7	74,5%	Verificación de los registros de autorización
5.3.8	74,0%	Verificación de cuentas y privilegios de acceso
8.3.3	54,7%	Registro de cambios del procedimiento de recuperación
8.3.4	78,9%	Respaldos y almacenamiento de información
8.3.5	58,8%	Registro de pruebas a los respaldos
9.3.3	69,0%	Registro de cambios del procedimiento respuesta a incidentes
7.3.2	80,7%	Herramientas de prevención de malware
Auditoría	76,0%	Desarrollo primera auditoría interna (entre el mes de **octubre de 2021** y el mes de **abril del 2022**).
50%	76,7%	Para el 50% de sus ciberactivos críticos (42m)
75%	65,7%	Para el 75% de sus ciberactivos críticos (54m)
100%	54,1%	Para el 100% de sus ciberactivos críticos (60m)

Mapa de Actividades Acuerdo 1502

Plan de sensibilización y entrenamiento para el personal relacionado con ciberactivos

Plan de gestión de incidentes de ciberseguridad

REPORTE DE AVANCE (%) - SEGUIMIENTO SEMESTRAL ACUERDO CNO 1502							
oct-20	77,5%	12 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).					
Num	**2020 (23) A.1241**	**2021 (22) A.1347**	**2022-I (24)**	**2022-II (31)**	**2023-I (41)**		**Actividad**
5.3.1	89,3%	98,9%	99,8%	87,5%	85,0%	↓	Política y lineamiento de ciberseguridad
5.3.4	32,8%	75,5%	69,2%	85,0%	87,6%	↑	Programa de conciencia de seguridad
5.3.5	27,2%	62,7%	73,9%	80,1%	79,6%	↓	Programa de entrenamiento y capacitación
9.3.1	57,4%	77,7%	90,8%	80,9%	79,0%	↓	Plan de respuesta ante incidentes
9.3.2	38,0%	57,7%	71,4%	62,2%	64,8%	↑	Documentación de pruebas o simulacros
9.3.3	20,0%	20,9%	62,8%	70,2%	69,0%	↓	Registro de cambios del procedimiento respuesta a incidentes

REPORTE DE AVANCE (%) - SEGUIMIENTO SEMESTRAL ACUERDO CNO 1502							
abr-21	93,5%	18 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).					
Num	**2020 (23) A.1241**	**2021 (22) A.1347**	**2022-I (24)**	**2022-II (31)**	**2023-I (41)**		**Activi**
5.3.2	100,0%	100,0%	96,8%	93,5%	93,5%	≈	Actulización responsable de ciberseguridad

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

Mapa de Actividades Acuerdo 1502

REPORTE DE AVANCE (%) - SEGUIMIENTO SEMESTRAL ACUERDO CNO 1502							
oct-22	74,1%	36 meses contados a partir del 3 de octubre de 2019 (el color indica su fecha máxima a cumplir 100%).					
Num	2020 (23) A.1241	2021 (22) A.1347	2022-I (24)	2022-II (31)	2023-I (41)		Actividad
Actualización de inventario de ciberactivos							
4.3.1	92,1%	95,9%	99,0%	89,0%	95,4%	↑	Activos críticos
4.3.2	74,8%	92,1%	94,2%	85,4%	92,0%	↑	Ciberactivos críticos
Seguridad electrónica de ciberactivos							
6.3.1	53,8%	80,0%	90,3%	83,9%	83,1%	↓	Perímetros de seguridad electrónica
5.3.7	22,5%	29,2%	60,1%	69,8%	74,5%	↑	Verificación de los registros de autorización
5.3.8	24,0%	31,5%	59,3%	73,8%	74,0%	↑	Verificación de cuentas y privilegios de acceso
5.3.9	30,9%	48,4%	75,6%	78,9%	77,4%	↓	Procedimiento de revocación de accesos
7.3.1	30,2%	39,5%	71,2%	73,4%	70,0%	↓	Procedimiento de control de cambios y gestión de configuraciones
7.3.2	51,8%	53,7%	69,7%	79,6%	80,7%	↑	Herramientas de prevención de malware
7.3.3	43,4%	65,0%	80,1%	73,9%	75,4%	↑	Procedimiento de evaluación de vulnerabilidades
7.3.4	32,4%	40,8%	77,3%	72,5%	69,7%	↓	Procedimiento de control ciberactivos críticos transitorios y medios extraíbles
7.3.5	35,0%	37,0%	78,3%	73,7%	66,7%	↓	Procedimiento de actualizaciones y parches de seguridad
Seguridad física para ciberactivos							
10.3.1	46,4%	54,5%	81,8%	78,5%	82,1%	↑	Plan de seguridad física
10.3.3	49,6%	66,7%	85,6%	84,1%	85,5%	↑	Procedimiento de control de visitantes
10.3.4	35,0%	42,0%	71,2%	68,0%	69,1%	↑	Procedimiento de mantenimiento y pruebas
Recuperación para ciberactivos							
8.3.1	22,8%	65,5%	76,4%	78,4%	76,9%	↓	Plan de recuperación y resiliencia
8.3.2	22,0%	47,7%	58,0%	61,0%	60,9%	↓	Plan de pruebas o simulacros
8.3.3	16,4%	24,9%	37,1%	60,6%	54,7%	↓	Registro de cambios del procedimiento de recuperación y resiliencia
8.3.4	33,4%	38,8%	60,9%	81,1%	78,9%	↓	Respaldos y almacenamiento de información
8.3.5	20,6%	30,6%	48,8%	62,3%	58,8%	↓	Registro de pruebas a los respaldos y mecanismos de contingencia y continuidad
Primera ejecución del plan de sensibilización y entrenamiento							
5.3.4	32,8%	75,5%	69,2%	85,0%	87,6%	↑	Primera ejecución Programa de conciencia de seguridad
5.3.5	27,2%	62,7%	73,9%	80,1%	79,6%	↓	Primera ejecución Programa de entrenamiento y capacitación
Implementación de los controles en los perímetros de seguridad							
6.3.1	37,8%	51,5%	77,1%	84,1%	79,3%	↓	Perímetros de seguridad electrónica
6.3.2	15,3%	33,4%	74,5%	81,9%	75,2%	↓	Listas de acceso
6.3.5	14,7%	34,2%	67,6%	66,2%	66,5%	↑	Procedimiento para habilitar los puntos de acceso
6.3.6	12,3%	34,5%	62,6%	71,7%	68,8%	↓	Procedimiento para la administración de conexiones temporales
6.3.7	16,6%	26,7%	60,3%	63,2%	62,7%	↓	Sistema de control intermedio
10.3.2	32,0%	32,6%	63,4%	78,0%	79,2%	↑	Restricción de acceso físico
Implementación de monitoreo básico de eventos							
6.3.3	26,9%	27,6%	82,4%	68,1%	69,1%	↑	Procedimiento de monitoreo y registro de acceso
7.3.6	23,6%	36,5%	70,8%	67,9%	68,0%	↑	Procedimiento para identificar y monitorear eventos
Gestión y evaluación ciberseguridad							
11.3.1	20,4%	29,8%	51,2%	63,6%	62,1%	↓	Plan de gestión de riesgo de la cadena de suministro (actualizado máximo a 24 meses)
5.3.3	37,9%	47,7%	85,6%	73,6%	73,0%	↓	Evaluación personal y riesgos
-	53,7%	72,8%	89,5%	76,5%	72,3%	↓	Actualización del nivel de gestión de ciberseguridad (análisis de brecha frente a la guía)
-	50,2%	77,2%	84,6%	72,7%	74,8%	↑	Actualización del análisis de riesgos y vulnerabilidades

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

Mapa de Actividades
Acuerdo 1502

REPORTE DE AVANCE (%) - SEGUIMIENTO SEMESTRAL ACUERDO CNO 1502	
-	Documentación (revisar, actualizar y conservar información soporte 3 años)
abr-22	Desarrollo primera auditoría interna (entre el mes de octubre de 2021 y el mes de abril del 2022).
abr-23	Para el 50% de sus ciberactivos críticos - (42) cuarenta y dos meses contados a partir del 3 de octubre de 2019.
abr-24	Para el 75% de sus ciberactivos críticos - (54) cuarenta y dos meses contados a partir del 3 de octubre de 2019.
oct-24	Para el 100% de sus ciberactivos críticos - (60) cuarenta y dos meses contados a partir del 3 de octubre de 2019.

Num	2020 (23) A.1241	2021 (22) A.1347	2022-I (24)	2022-II (31)	2023-I (41)		Actividad
3	26,5%	27,8%	72,7%	72,7%	73,6%	↑	Cumplimiento (revisar, actualizar y conservar información soporte, 3años)
Auditoría			89,0%	81,5%	76,0%	↓	Desarrollo primera auditoría interna (Oct-2021 - abr-2022)
50%		32,3%	69,1%	74,1%	76,7%	↑	Para el 50% de sus ciberactivos críticos (42m)
75%			46,1%	58,5%	65,7%	↑	Para el 75% de sus ciberactivos críticos (54m)
100%			32,2%	50,6%	54,1%	↑	Para el 100% de sus ciberactivos críticos (60m)

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

Evaluación de la madurez en ciberseguridad

Criterios

1

Alineación

Regulación y acuerdos existentes

2

Esfuerzo sectorial

Motivar la participación de las empresas (actor para implementar el ejercicio, costo y duración)

3

Agilidad

Oportunidad para desarrollar un ejercicio sectorial y en el marco del plan de acción sectorial 2023

Instrumento

1

Estado de implementación de prácticas de ciberseguridad

NIST CYBERSECURITY FRAMEWORK (CSF) IDENTIFY PROTECT DETECT RESPOND RECOVER **CSF 1.1-108**

2

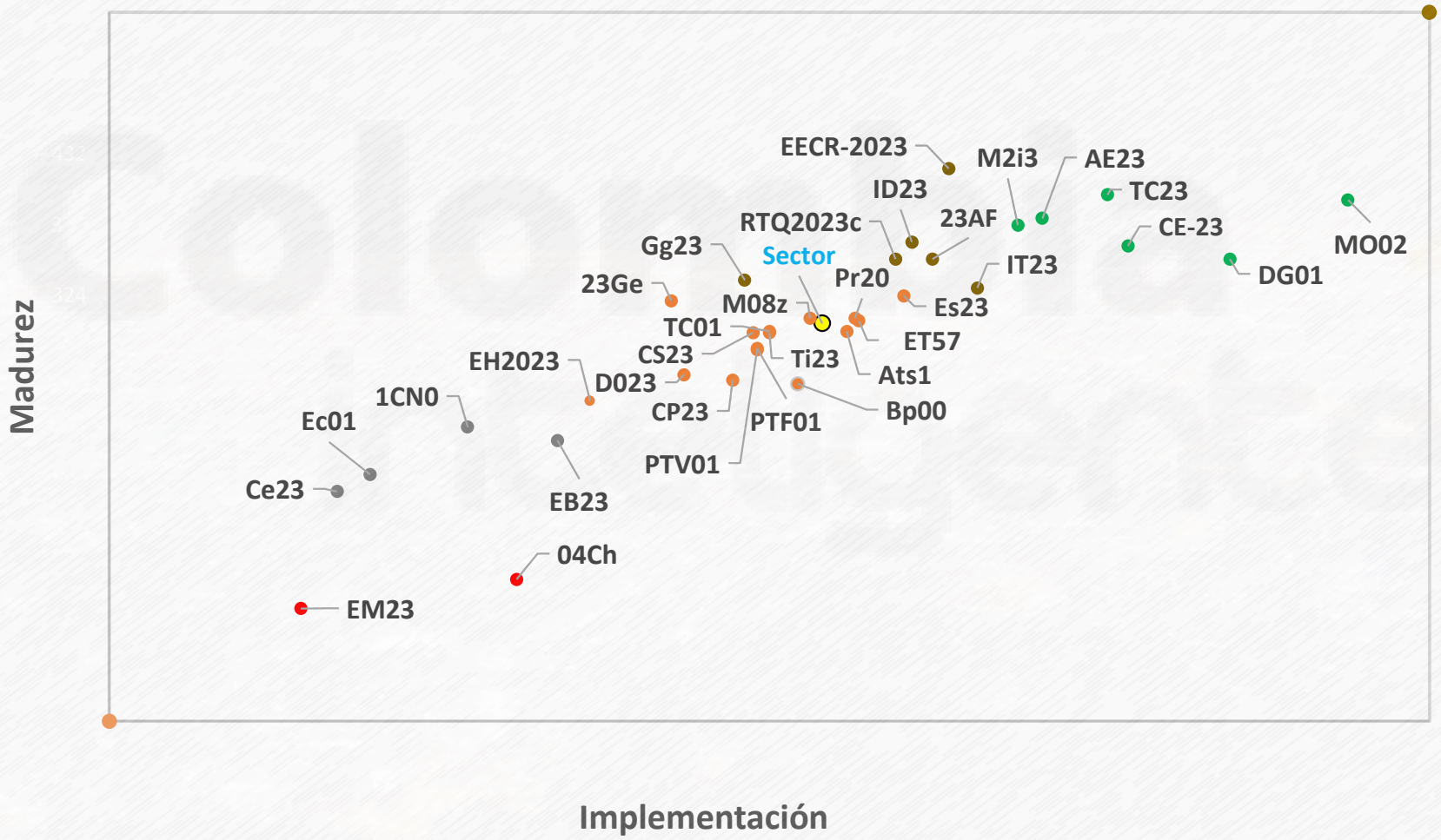
Estado de madurez de las prácticas NIST-CSF 1.1-108

National Association Regulatory Utility Commissioners

3

Mapeo sectorial prácticas ciberseguridad (implementación, madurez)

Mapeo sectorial - 2023



Zona 0
No deseada

Zona 1
Baja implementación o madurez

Zona 2
Fortalecer implementación y madurez

Zona 3
Fortalecer implementación o madurez

Zona 4
Implementación y madurez deseable

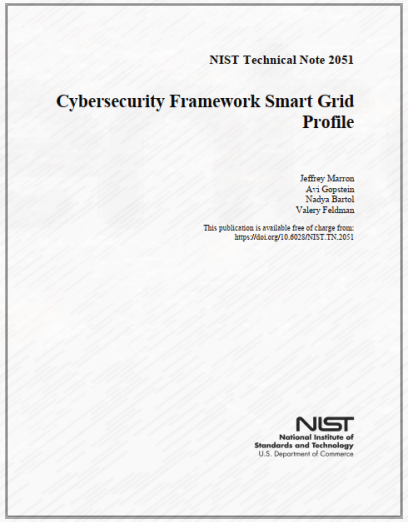
Zona 5
Alta implementación y madurez

Perfil ciberseguridad

Función	Categorías	# Prácticas	Perfil 1 2 3 4 5 6 7 8 9 10 11 12
Identificar	Gestión de Activos	6	
	Entorno de Negocios	5	
	Gobernanza	4	
	Evaluación del riesgo	6	
	Estrategia de gestión del riesgo	3	
	Gestión de la cadena de suministro	5	
Proteger	Control de acceso	7	
	Entrenamiento y conciencia situaciona	5	
	Seguridad de datos	8	
	Procesos/procedimientos protección Ir	12	
	Mantenimiento	2	
	Tecnologías de protección	5	
Detectar	Eventos y anomalías	5	
	Monitoreo continuo de la seguridad	8	
	Procesos de detección	5	
Responder	Planeación de la respuesta	1	
	Comunicación de la respuesta	5	
	Análisis	5	
	Mitigación	3	
	Mejoras	2	
Recuperar	Planeación de la recuperación	1	
	Comunicación de la recuperación	2	
	Mejoras	3	

Prácticas de ciberseguridad para fortalecer las acciones en:

Confiabilidad
Seguridad
Modernización
Resiliencia


NIST Technical Note 2051

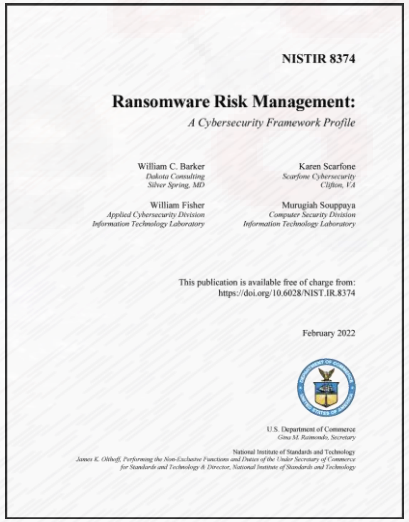
Cybersecurity Framework Smart Grid Profile

Jeffrey Marron
Avi Gopstein
Nadya Bartol
Valery Feldman

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2051

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Ransomware


NISTIR 8374

Ransomware Risk Management:
A Cybersecurity Framework Profile

William C. Barker
Dakota Consulting
Silver Spring, MD

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

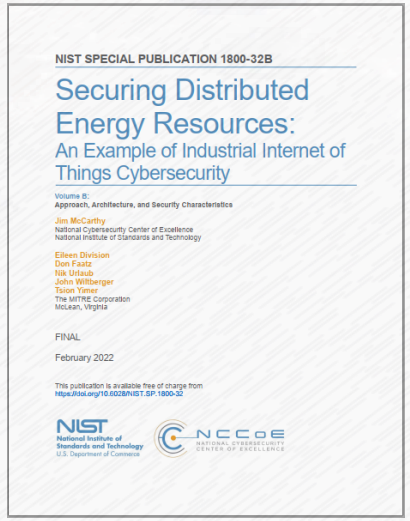
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374

February 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

DER


NIST SPECIAL PUBLICATION 1800-32B

Securing Distributed Energy Resources:
An Example of Industrial Internet of Things Cybersecurity

Volume B:
Approach, Architecture, and Security Characteristics

Jim McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Eileen Division
Don Faatz
Nik Urlaub
John Wiltberger
Tsion Yimer
The MITRE Corporation
McLean, Virginia

FINAL

February 2022

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-32

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

PERFIL DE PRÁCTICAS EN CIBERSEGURIDAD

Función	Categorías	Gestión riesgo Ransomware	Soportar la modernización	Mantener la resiliencia	Mantener la confiabilidad	Mantener la seguridad	Control de seguridad DER
Identificar	Gestión de Activos						
	Entorno de Negocios						
	Gobernanza						
	Evaluación del riesgo						
	Estrategia de gestión del riesgo						
	Gestión de la cadena de suministro						
Proteger	Control de acceso						
	Entrenamiento y conciencia situacional						
	Seguridad de datos						
	Procesos/procedimientos protección Inf						
	Mantenimiento						
	Tecnologías de protección						
Detectar	Eventos y anomalías						
	Monitoreo continuo de la seguridad						
	Procesos de detección						
Responder	Planeación de la respuesta						
	Comunicación de la respuesta						
	Análisis						
	Mitigación						
	Mejoras						
Recuperar	Planeación de la recuperación						
	Comunicación de la recuperación						
	Mejoras						

PERFIL DE PRÁCTICAS EN CIBERSEGURIDAD (implementación)

0. No implementada
1. Parcialmente implementada
2. Ampliamente implementada
3. Completamente implementada

Función	Categorías - Implementación	Gestión riesgo Ransomware	Soportar la modernización	Mantener la resiliencia	Mantener la confiabilidad	Mantener la seguridad	Control de seguridad DER
Identificar	AM. Gestión de Activos						
	BE. Entorno de Negocios						
	GV. Gobernanza						
	RA. Evaluación del riesgo						
	RM. Estrategia de gestión del riesgo						
	SC. Gestión de la cadena de suministro						
Proteger	AC. Control de acceso						
	AT. Entrenamiento y conciencia situacior						
	DT. Seguridad de datos						
	IP. Procesos/procedimientos protección						
	MA. Mantenimiento						
	PT. Tecnologías de protección						
Detectar	AE. Eventos y anomalías						
	CM. Monitoreo continuo de la seguridad						
	DP. Procesos de detección						
Responder	RP. Planeación de la respuesta						
	CO. Comunicación de la respuesta						
	AN. Análisis						
	MI. Mitigación						
	IM. Mejoras						
Recuperar	RP. Planeación de la recuperación						
	IM. Mejoras						
	CO. Comunicación de la recuperación						

Implementación

0 **2** **3**

PERFIL DE PRÁCTICAS EN CIBERSEGURIDAD (madurez)

0. Sin criterio
1. Sin información
2. Inicial
3. Establecida
4. Madura
5. Optimizada

Función	Categorías - Madurez	Gestión riesgo Ransomware	Soportar la modernización	Mantener la resiliencia	Mantener la confiabilidad	Mantener la seguridad	Control de seguridad DER
Identificar	AM. Gestión de Activos						
	BE. Entorno de Negocios						
	GV. Gobernanza						
	RA. Evaluación del riesgo						
	RM. Estrategia de gestión del riesgo						
	SC. Gestión de la cadena de suministro						
Proteger	AC. Control de acceso						
	AT. Entrenamiento y conciencia situacior						
	DT. Seguridad de datos						
	IP. Procesos/procedimientos protección						
	MA. Mantenimiento						
	PT. Tecnologías de protección						
Detectar	AE. Eventos y anomalías						
	CM. Monitoreo continuo de la seguridad						
	DP. Procesos de detección						
Responder	RP. Planeación de la respuesta						
	CO. Comunicación de la respuesta						
	AN. Análisis						
	MI. Mitigación						
	IM. Mejoras						
Recuperar	RP. Planeación de la recuperación						
	IM. Mejoras						
	CO. Comunicación de la recuperación						

Madurez

0 **3** **5**

Trabajo continuo …

1. Garantizar el **reporte** de todos los agentes responsables de ciberseguridad (requerimiento CNO) e implementar mapa de avance por activos críticos (Anexo 1)

2. **Armonizar** el **nivel de avance** en ciberseguridad y promover la **estandarización** para mitigar brechas existentes

3. **Empoderar** la gestión de ciberseguridad a **todo nivel jerárquico** (procesos organizacionales: administración, planeación, operación, mantenimiento, regulación, …) para fortalecer el aprendizaje, articulación y colaboración sectorial

Presidencia

Presidente - Jaime A. Zapata U. (XM)
Vicepresidente – Alberto Olarte A. (CNO)

Contacto

Juan D. Molina C. Ing. Electricista. D.Sc. M.Sc. Esp.
Líder de Gestión
juandavid.molina@colombiainteligente.org

Edf. TecnoParque, Piso 13. CIDET.
Carrera 46 # 56 – 11. CP:050012
Medellín, Colombia.
http://www.colombiainteligente.org/
@colombiaintelig

Seguiremos trabajando por la transformación del sector eléctrico !