Herramienta de armonización entre las normas 27001 y NIST-53 como pilares para la medición del nivel de madurez del SGSI. Diciembre de 2021

I. J. Zarate

Resumen – Las entidades que cuentan con un sistema de gestión de seguridad de la información basado en la norma NTC ISO/IEC 27001:2013, debe realizar un trabajo arduo para mantener las buenas practicas de seguridad que esta norma define, sin embargo esto no es suficiente para tener una seguridad integral entre los activos que se encuentran en el ciberespacio y los activos que se encentran on premise, por esta razón se desarrolla una herramienta que armoniza los controles de la norma ISO/IEC 27001:2013 y los controles del Framework de Ciberseguridad NIST 800-53 Rev 5. El objetivo del presente articulo es presentar el resultado de la herramienta de medición de la madurez de Seguridad de la Información y ciberseguridad en una compañía de telecomunicaciones de Colombia. Al utilizar la herramienta de medición de madurez se puede identificar la calificación de los requisitos y dominios del anexo A la norma ISO/IEC 27001:2013 y los controles del Framework de Ciberseguridad NIST 800-53. El presente trabajo aporta con el desarrollo de la herramienta de medición de la madurez de Seguridad de la Información, la cual puede ser utilizada en cualquier compañía que requiera medir el nivel de madurez del SGSI. que se puede utilizar

Palabras Claves – ISO/IEC 27001:2013, NIST SP 800-53 v5, Madurez, Ciberseguridad

Abstract - The entities that have an information security management system based on the NTC ISO/IEC 27001:2013 standard, must make an arduous work to maintain good security practices that this standard defines, however this is not enough to have a comprehensive security between the assets that are in cyberspace and the assets that are on premise, for this reason a tool that harmonizes the controls of the ISO/IEC 27001:2013 standard and the controls of the Cybersecurity Framework NIST 800-53 Rev 5 is developed. The objective of this article is to present the results of the Information Security and Cybersecurity maturity measurement tool in a telecommunications company in Colombia. By using the maturity measurement tool it is possible to identify the qualification of the requirements and domains of Annex A of the ISO/IEC 27001:2013 standard and the controls of the NIST 800-53 Cybersecurity Framework. The present work contributes with the development of the Information Security maturity measurement tool, which can be used in any company that requires to measure the ISMS maturity level. that can be used

Keywords - ISO/IEC 27001:2013, NIST SP 800-53 v5, Maturity, Cybersecurity

I. INTRODUCCION

Las ciberamenazas aumentan de manera exponencial, poniendo en riesgo la información de las compañías, por esta razón las empresas buscan la manera de proteger su activo más importante, para salvaguardar la información privada y confidencial, las empresas implementan la Norma NTC ISO/IEC 27001:2013 Requisitos del Sistema de Gestión de Seguridad de la Información, sin embrago, aunque se implemente este sistema de gestión en las compañías, no mitiga los riesgos asociados a la Ciberseguridad en un 100%.

Para mitigar los Ciberriesgos, The National Institute of Standars and Tecnology NIST liberó los controles que se encuentran en su publicacion especial SP NIST 800-53 Security and Privacy Controls for Information Systems and Organizations que al implementarse, gestionarse y monitorearse ayudan a mitigar los riesgos que pueden afectar la Confidencialidad, Integridad y Disponibilidad de la información.

Si las empresas miran la seguridad como un gran universo el cual está conformado por la Ciberseguridad, Seguridad Informática y Seguridad de la información, y no se ven como islas, se puede obtener una empresa con un nivel de seguridad y Ciberseguridad muy robusto.

Para medir la madurez del sistema de Seguridad y Ciberseguridad de las organizaciones requiere realizar una evaluación integral del estado actual de la seguridad y Ciberseguridad de las compañías, por esta razón se crea una herramienta que pueda ayudar a identificar las brechas en cada uno de los controles.

II. La Ciberseguridad en los últimos años

En el último año se han presentado gran cantidad de cambios de nuestro diario vivir por la situación presentada a raíz de la pandemia, por tal razón los cibercriminales han aprovechado esta situación para intensificar sus acciones delictivas.

Según el reporte de la INTERPOL[1] Ciberdelincuencia: Efectos de la Covid-19, los cibercriminales realizaron cambios en sus métodos de ataques y de objetivos, con el fin de ampliar el alcance de sus ataques, para poder obtener más ingresos económicos.

La dirección de Ciberdelincuencia de INTERPOL utiliza la información obtenida en los 194 países miembros y de sus socios privados para determinar la siguiente información.

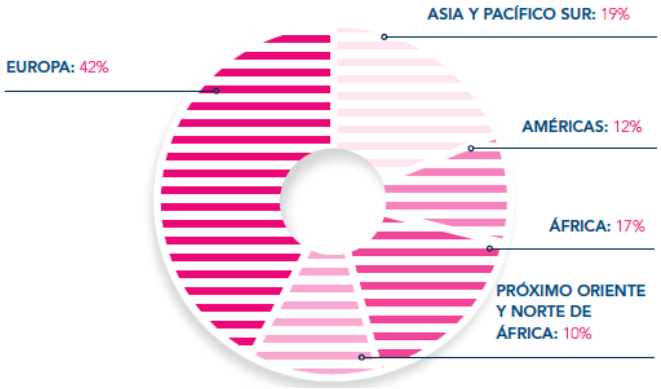

Fig. 1 Encuesta mundial de INTERPOL sobre ciberdelincuencia - Distribución por regiones de los países que han respondido

De los países que enviaron información a la INTERPOL, en la Fig. 1 del reporte Ciberdelincuencia: Efectos de la Covid-19 se puede evidencia los continentes y se porcentaje de ataques que han sufrido cada uno estos. Ubicando en primer lugar a Europa con un 42% de ataques, de segundo lugar se encuentra Asia y Pacifico Sur, con un 19%. En un 17% se encuentra el continente africano, América se encuentra en un 4to lugar con un 12% del total de los Ciberdelitos y por último lugar se encuentra Próximo Oriente norte de África con un 10%.

En el reporte de la INTERPOL se encuentran la distribución de los ataques que utilizaron los ciberdelincuentes, en ataque más utilizado fue el phishing, en segundo lugar, se encuentra el Malware o Ransomware, en tercer lugar, se encontraban los dominós maliciosos, y por último se encuentran las noticias falsas, como se puede ver en la Fig. 2 a continuación.

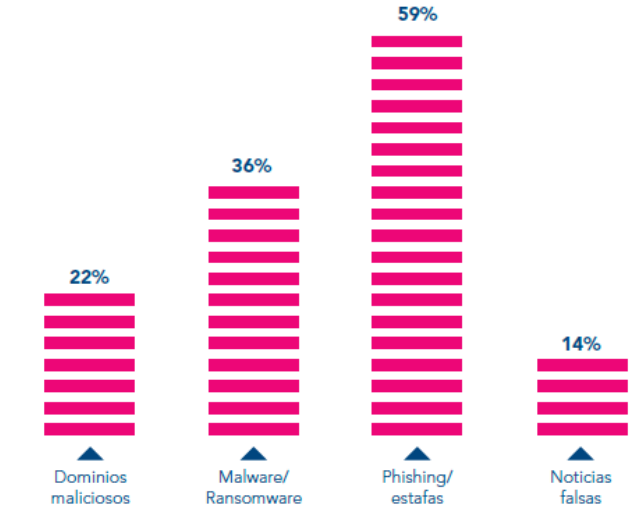

Fig. 2 Proporción de las principales ciberamenazas relacionadas con la COVID-19 calculada a partir de la información dada por los países miembros

Colombia no está exento de estas ciberamenazas, al contrario de pensar que esta fuera de los ojos de los cibercriminales, Colombia se encuentra en el tercer lugar de los países más atacados de acuerdo con el informe generado por TrendMicro Colombia es el tercer país más atacado con 462005 ciberataques ubicándolo por debajo de Estados Unidos y Alemania.

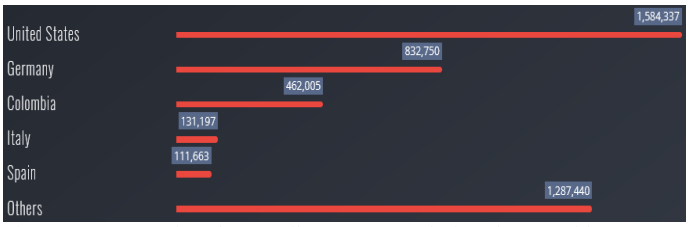

Fig. 3 Top países afectados por ciberamenazas relacionadas a Covid-19

En Colombia en el año 2019 se identificaron diversos Ataques BEC[2], los cuales dividen en los siguientes vectores de ataques: 80% Spear-Phishing o Correos Fraudulentos dirigidos a un objetivo específico. En un 60% hace referencia a la suplantación de identidad de una persona o empresa. En tercer lugar, se encuentra el Spoofing de correo, el cual realiza enmascaramiento de correos con el fin de engañar al usuario final, y en un 37% se generaron infecciones de sitios frecuentemente visitados por empleados.

El Ataque BEC en el 2018 el FBI informa que se generaron perdidas globales por un valor de hasta 12.000 millones de dólares, sin embargo, en Colombia, se presentaron perdidas que pueden oscilar entre 300 millones de pesos y 5000 millones de pesos, de acuerdo con el tamaño de la empresa que sufrió el ataque.

El ransomware es una amenaza que amenaza a todos las personas, empresas y gobiernos por igual. Para el 2019 Colombia estaba en la mira de los ciberdelincuentes, ya que recibió el 30% de los ataques realizados en Latinoamérica,

[1] La Organización Internacional de Policía Criminal (INTERPOL)

[2] Business Email Compromise

seguidos por Perú con un 16% de los ataques, México un 14%, Brasil y Argentina con un 11% y 9% respectivamente.

En el informe de tendencias Cibercrimen Colombia 2019-2020, se evidencia que el 83% de las empresas carecen de protocolos de respuesta a incidentes de Seguridad de la Información.

Otro vector de ataque que se presenta en el informe de tendencias Cibercrimen Colombia 2019 – 2020 hace referencia a la infección de Malware en los activos o red de la compañía. El incremento de infección por programas malicioso en Colombia sufrió un incremento del año 2019.

De acuerdo con lo informado en los párrafos anteriores, se plantea la siguiente metodología para el desarrollo de la herramienta de medición.

III. METODOLOGIA

Como punto de arranque se inicia con la identificación de las familias de los controles de la NIST SP 800-53 y los dominios del Anexo A de la Norma ISO/IEC 27001:2013, al mismo tiempo para poder determinar un nivel de madurez de Seguridad y Ciberseguridad en las compañías es necesario contar con una herramienta que ayude a identificar las brechas de Seguridad y Ciberseguridad, para ello esto se puede definir un nivel de clasificación de la madurez de la compañía, adaptando el nivel del modelo de capacidad de procesos que está incluido en la metodología de COBIT 5.

Como resultado se define los criterios y niveles de madurez.

1. Nivel Incompleto, otorgándole una clasificación de 0 a 0,9
2. Nivel Ejecutado, esto quiere decir que el control se encuentra implementado y realiza de manera adecuada su función, si el control se encuentra en este nivel se le otorgará un nivel de 1 a 1.9.
3. Nivel Gestionado: esto quiere decir que el control ya está implementado y se le realiza una gestión planificada, una revisión de este y se ajustan desviaciones que puedan ocurrir. La calificación que se le otorga a los controles que se encuentren en este nivel es valor de 2 a 2,9.
4. Nivel Establecido: Para establecer un nivel de madurez Establecido, todos los controles y requisitos deben ser evaluados y deben contar con una prueba de recorrido por medio de un proceso de auditoria interno o externo, la calificación esta entre 3,0 a 3,9.
5. Nivel Predecible: Para establecer un nivel de madurez predecible se debe contar con un monitoreo y acciones frente a los monitoreos e indicadores gestionados, la calificación de madurez para llegar a este nivel debe estar entre 4,0 a 4,9.
6. Nivel Optimizado: Para establecer el nivel de madurez de optimizado, se debe automatizar los procesos para que no se generen errores, para obtener este nivel de madurez todos los controles deben tener una calificación igual a 5,0.

Fig. 4. Niveles de Seguridad de acuerdo con el COBIT 5

A partir del levantamiento de información en donde se identifica la información relevante que se requiere para determinar el tipo de herramienta a desarrollar, los campos y criterios de evaluación que se van a revisar en cada uno de los controles de la norma ISO/IEC 27001:2013 y los controles del Framework de Ciberseguridad NIST SP 800-53.

A continuación del levantamiento de información se procede a seleccionar la metodología de medición, si es cuantitativa, cualitativa y/o mixta, esto con el fin dar una calificación exacta del nivel de madurez de las organizaciones.

Una vez se tiene definido los criterios y la metodología de evaluación, se procede a realizar el diseño y creación de la herramienta, que se ayudará a definir el nivel de madurez de Seguridad de la Información y Ciberseguridad de las organizaciones.

Una vez la herramienta se encuentre desarrollada en su totalidad se procede a realizar la evaluación de madurez en la empresa Partners Telecom Colombia, con los resultados obtenidos en esta fase, se procede a realizar ajustes a las desviaciones evidenciadas en el ejercicio.

Después de que se cuente con la herramienta ajustada se procede generar oportunidades de mejora y recomendaciones para incrementar el nivel de madurez en la organización.

IV. ARMONIZACIÓN DE LOS CONTROLES DE LOS CONTROLES DE SEGURIDAD Y CIBERSEGURIDAD

Adicional a la definición de una calificación, se debe realizar un mapeo de los controles que contiene el framework de Ciberseguridad y los controles que se encuentran definidos en el anexo A de la norma del Sistema de Gestión de Seguridad de la Información ISO/IEC 27001:2013 para lo cual se utilizan el documento que se encuentra en publicado en la página de la NIST, en el cual se armonizan los controles de la Norma ISO 27001 del 2013 con los controles de la NIST SP 800-53.

Función	Control NIST	Control Anexo A 27001
IDENTIFY (ID)	ID.AM	A.8.1.1 - A.8.1.2 - A.8.1.1 - A.8.1.2 - A.13.2.1 - A.11.2.6 - A.8.2.1 - A.6.1.1
	ID.BE	A.15.1.3 - A.15.2.1 - A.15.2.2 - R.4.1 - R.5.1 - R.5.2 - R.6.2 - R.7.4 - A.11.2.2 - A.11.2.3 - A.12.1.3 - A.11.1.4 - A.17.1.1 - A.17.1.2 - A.17.2.1
	ID.GV	A.5.1.1 - A.6.1.1 - A.7.2.1 - A.18.1.1 - R.6.1.1 - R.6.1.2 - R.6.1.3 - R.8.2 - R.8.3
	ID.RA	A.12.6.1 - A.18.2.3 - A.6.1.4 - R.4.1 - R.6.1.1 - R.6.1.2 - A.12.6.1
	ID.RA	R.6.1.1 - R.6.1.2 - R.6.1.3 - R.6.1.1 - R.6.1.1
PROTECT (PR)	PR.AC	A.9.2.1 - A.9.2.2 - A.9.2.4 - A.9.3.1 - A.9.4.2 - A.9.4.3 - A.11.1.1 - A.11.1.2 - A.11.1.4 - A.11.1.6 - A.11.2.3 - A.6.2.2 - A.13.1.1 - A.13.2.1 - A.6.1.2 - A.9.1.2 - A.9.2.3 - A.9.4.1 - A.9.4.4 - A.13.1.1 - A.13.1.3 - A.13.2.1
	PR.AT	A.7.2.2 - A.6.1.1 - A.7.2.2 - A.6.1.1 - A.7.2.2 - A.6.1.1 - A.7.2.2 - A.6.1.1 - A.7.2.2
	PR.DS	A.8.2.3 - A.8.2.3 - A.13.1.1 - A.13.2.1 - A.13.2.3 A.14.1.2 - A.14.1.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.8.3.3 - A.11.2.7 - A.12.3.1 - A.6.1.2 - A.7.1.1 - A.7.1.2 - A.7.3.1 - A.8.2.2 - A.8.2.3 - A.9.1.1 - A.9.1.2 - A.9.2.3 - A.9.4.1 - A.9.4.4 - A.9.4.5 - A.13.1.3 - A.13.2.1 - A.13.2.3 - A.13.2.4 - A.14.1.2 - A.14.1.3 - A.12.2.1 - A.12.5.1 - A.14.1.2 - A.14.1.3 - A.12.1.4
	PR.IP	A.12.1.2 - A.12.5.1 - A.12.6.2 - A.14.2.2 - A.14.2.3 - A.14.2.4 - A.6.1.5 - A.14.1.1 - A.14.2.1 - A.14.2.5 - A.12.1.2 - A.12.5.1 - A.12.6.2 - A.14.2.2 - A.14.2.3 - A.14.2.4 - A.12.3.1 - A.17.1.2 - A.17.1.3 - A.18.1.3 - A.11.1.4 - A.11.2.1 - A.11.2.2 - A.11.2.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.11.2.7 - R.10.2 - A.16.1.6 - A.16.1.1 - A.17.1.1 - A.17.1.2 - A.17.1.3 - A.7.1.1 - A.7.3.1 - A.8.1.4 - A.12.6.1 - A.18.2.2
	PR.MA	A.11.1.2 - A.11.2.4 - A.11.2.5 - A.11.2.4 - A.15.1.1 - A.15.2.1
	PR.PT	A.12.4.1 - A.12.4.2 - A.12.4.3 - A.12.4.4 - A.12.7.1 - A.8.2.2 - A.8.2.3 - A.8.3.1 - A.8.3.3 - A.11.2.9 - A.9.1.2 - A.13.1.1 - A.13.2.1
DETECT (DE)	DE.AE	A.12.6.2 - A.13.1.1 - A.13.1.2 - A.13.1.3 - A.16.1.1 - A.16.1.4 - A.16.1.2 - A.16.1.4 - A.16.1.4
	DE.CM	A.13.1.2 - A.11.1.1 - A.11.1.2 - A.11.1.3 - A.11.1.4 - A.12.4.1 - A.12.2.1 - A.12.5.1 - A.14.2.7 - A.15.2.1 - A.11.2.1 - A.12.6.2 - A.13.1.2 - A.12.6.1
	DE.DP	A.6.1.1 - A.18.1.4 - A.14.2.8 - A.16.1.2 - A.16.1.6
RESPOND (RS)	RS.RP	A.16.1.5
	RS.CO	A.6.1.1 - A.16.1.1 - A.6.1.3 - A.16.1.2 - A.16.1.2 R.9.3 - R.7.4
	RS.AN	A.12.4.1 - A.12.4.3 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.16.1.4
	RS.MI	A.16.1.5 - A.12.2.1 - A.16.1.5 - A.12.6.1
	RS.IM	A.16.1.6
RECOVER (RC)	RC.RP	A.16.1.5
	RC.IM	A.16.1.6 - A.16.1.5
	RC.CO	R.7.4 - A.6.1.3 - A.6.1.4 - R.7.4 - R.7.4 - A.6.1.5

Tabla 1 Integración de los controles ISO/EC 27001:2013 VS NIST 800.53 V5

En la Tabla 1 se evidencia la relación de los requisitos y los controles del Anexo A de la norma de *Sistema de Gestión de Seguridad de la Información* ISO/IEC 27001:2013 y los controles del Framework de Ciberseguridad NIST SP 800-53 Rev.5 *Security and Privacy Controls for Information Systems and Organizations.*

Una vez se definió la armonización de los controles de las normas de seguridad y ciberseguridad, se continua con la siguiente fase de ejecución la cual consiste en el desarrollo de la herramienta de medición de la madurez del sistema de gestión.

V. Desarrollo de la Herramienta de Medición.

El input de inicio de esta fase consistió en el resultado de los controles correlacionados entre sí, a continuación, se procede a definir los aspectos que se van a evaluar, en este caso se utilizan 6 aspectos y cada uno de estos cuenta con subniveles los cuales se mencionan a continuación:

1. Existencia: En este aspecto se evalúa que exista el control sin tener en cuenta que este documentado o no este documentado
    a. Si: En el proceso de la evaluación se valida que el requerimiento o el control del anexo A se esté ejecutando en la compañía.
    b. No: Se selecciona esta opción si no se está ejecutando el requerimiento o el control en la compañía.

2. Doc_Proceso: En este aspecto se evalúa que el requerimiento o control se encuentre documentado, ya sea este o no este formalizado, divulgado, o evaluado.
    a. No Formalizado: Se tiene documentado el control, pero está fuera de los estándares definidos por la organización.
    b. Formalizado: Se tiene documentado el control o el requerimiento y están formalizado en los sistemas de gestión de la organización.
    c. Divulgado: El control o requisito es divulgado a las partes interesadas al interior y/o exterior de la organización.
    d. Evaluado: Se revisa que las partes interesadas realicen las evaluaciones de los requisitos o controles previamente divulgados.

3. Prueba de Recorrido: En este aspecto de evaluación de espera que la organización se realice un proceso de auditoria interno o externo que abarque todos los requerimientos y controles de la 27001:2013
    a. Si: Se ha realizado un proceso formal y documentado de auditoría a los requerimientos y controles de la Norma ISO 27001:2013.
    b. No: Nunca se ha realizado un proceso formal y documentado de auditoría a los requerimientos y controles de la Norma ISO 27001:2013

4. Monitoreo: Se debe contar con un proceso formal de monitoreo a los requisitos y controles de la Norma ISO 27001:2013, con el fin de identificar posibles incidentes.
    a. Si - No se toman acciones: se debe seleccionar esta opción si se identifica que los monitoreos que se cuentan para los controles o requerimientos no surten efecto y se presentan incidentes.
    b. Si - Se toman acciones: se debe seleccionar esta opción si se identifica que los monitoreos son efectivos y si se identifican alertas se realiza un proceso de control de acuerdo con lo documentado.
    c. No: Se debe seleccionar esta opción al no contar con monitoreos para los requisitos o controles de la organización.

5. Indicadores: Se debe contar con un proceso formal de creación, diligenciamiento y mejora de los indicadores de acuerdo con lo definido por la organización.
    a. No definidos: Se debe seleccionar esta opción al no contar con indicadores de medición para los requisitos o controles de la organización.
    b. Medidos: se debe seleccionar esta opción si se identifica que los indicadores están medidos y no se toman acciones por las desviaciones.
    c. Gestionados: se debe seleccionar esta opción si se identifica que los indicadores están gestionados y si se presentan desviaciones se toman acciones correctivas y planes de mejora.

6. Tipo de Control: Este aspecto de medición hace referencia a la forma como se ejecuta el control
    a. Automático: Se debe selección esta opción si en la ejecución del control no interviene alguna persona.
    b. Semiautomático Se debe selección esta opción si en la ejecución del control se realiza de manera automática, pero interviene alguna persona.
    c. Manual: Se debe selección esta opción si en la ejecución del control lo ejecuta una persona.

Después de tener definido los niveles de madures y los criterios de evaluación se define la matriz de calificación en la cual se encuentra la escala de medición de los niveles de madurez vs los aspectos a evaluar, y las calificaciones que se obtienen con las diferentes combinaciones de las subcategorías.

Nivel de Madurez	Aspectos a Evaluar						Valor de Madurez
	Existencia	Proceso Documentado	Prueba Recorrido	Monitoreo	Indicadores	Tipo_Control	
Incompleto	No	-	-	-	-	-	0,00
Ejecutado	Si	No Formalizado	-	-	-	-	1,20
	Si	Formalizado	-	-	-	-	1,60
	Si	Divulgado	-	-	-	-	1,80
Gestionado	Si	Evaluado	No	-	-	-	2,00
Establecido	Si	Evaluado	Si	-	-	-	3,00
	Si	Evaluado	Si	No	-	-	3,00
	Si	Evaluado	Si	Si - No se toman acciones	-	-	3,06
	Si	Evaluado	Si	Si - Se toman acciones	-	-	3,50
	Si	Evaluado	Si	Si - Se toman acciones	No definidos	-	3,50
	Si	Evaluado	Si	Si - Se toman acciones	Medidos	-	3,60
Predecible	Si	Evaluado	Si	Si - Se toman acciones	Gestionados	-	4,00
	Si	Evaluado	Si	Si - Se toman acciones	Gestionados	Manual	4,33
	Si	Evaluado	Si	Si - Se toman acciones	Gestionados	Semiautomático	4,83
Optimizado	Si	Evaluado	Si	Si - Se toman acciones	Gestionados	Automatico	5,00

Tabla 2. Matiz Calificación

A continuación de tener la matriz de calificación, los criterios de evaluación y niveles de madures se realiza la construcción de la plantilla de evaluación.

La plantilla se divide en ocho partes las cuales se explican a continuación:

1. Título de la hoja a evaluar, puede ser los requisitos de la norma ISO/IEC 27001:2013 y/o controles del Anexo A de la Norma ISO/IEC 27001:2013.
2. Título del dominio o requisito puntual a evaluar.
3. Nombre del control o requisito puntual que se realiza la evaluación.
4. Descripción breve del control o requisito de la norma.
5. Se relacionan los controles de la NIST SP 800-53 que se mapean con los controles de la 27001:2013
6. La hoja cuenta con los aspectos a evaluar los cuales son los que se miden y generan el nivel de madurez.
7. La columna de Observaciones se utiliza para poner las recomendaciones y comentarios frente a las evaluaciones.
8. La columna nivel Madurez muestra el valor numérico de la calificación.

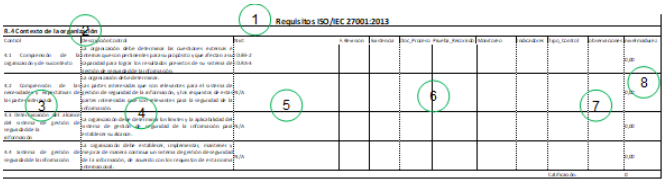

Tabla 3 Formato de Evaluación de la Madurez

Cuando se termina de diseñar el formato de evaluación de madurez se procede a crear las tablas y graficas que muestren el resultado obtenido por requisito, dominio o familia de controles. Para este fin se utilizaron graficas de barras y graficas radiales que ayudan a identificar el nivel de madurez.

Control	Calificación
R.4 Contexto de la organización	0,00
4.1 Comprensión de la organización y de su contexto	0,00
4.2 Comprensión de las necesidades y expectativas de las partes interesada	0,00
4.3 Determinación del alcance del sistema de gestión de seguridad de la información	0,00
4.4 Sistema de gestión de seguridad de la información	0,00
R.5 Liderazgo	0,00
5.1 Liderazgo y compromiso	0,00
5.2 Política	0,00
5.3 Roles, responsabilidades y autoridades en la organización	0,00
R.6 Planificación	0,00
6.1.1 Consideraciones generales	0,00
6.1.2 Apreciación de riesgos de seguridad de la información	0,00
6.1.3 Tratamiento de los riesgos de seguridad de la información	0,00
6.2 Objetivos de seguridad de la información y planificación para su consecución	0,00
R.7 Soporte	0,00
7.1 Recursos	0,00
7.2 Competencia	0,00
7.3 Concienciación	0,00
7.4 Comunicación	0,00
7.5.1 Consideraciones generales	0,00
7.5.2 Creación y actualización	0,00
7.5.3 Control de la información documentada	0,00
R.8 Operación	0,00
8.1 Planificación y control operacional.	0,00
8.2 Evaluación de riesgos de seguridad de la información.	0,00
8.3 Tratamiento de riesgos de seguridad de la información.	0,00
R.9 Evaluación del desempeño	0,00
9.1 Monitoreo, medición, análisis y evaluación	0,00
9.2 Auditoría interna	0,00
9.3 Revisión por la dirección	0,00
R.10 Mejora	0,00
10.1 No conformidad, acción correctiva	0,00
10.2 Mejora continua	0,00

Tabla 4 Resultados de los requisitos de la norma ISO/IEC 27001:2013

Fig. 5 Grafica Radial de la Madurez para los Requisitos del SGSI

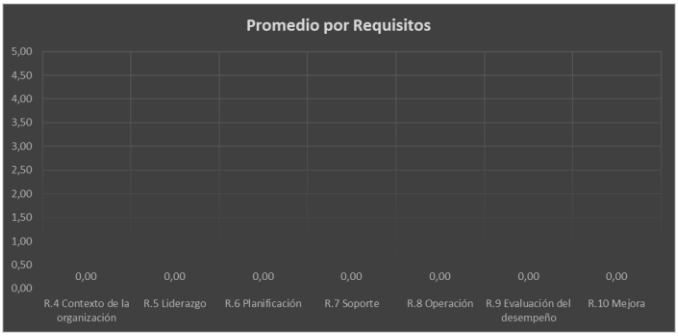

Fig. 6 Grafica de Barras de la Madurez para los Requisitos del SGSI

VI. Resultados Obtenidos

Al concluir el desarrollar la herramienta de medición de madurez, se procede a realizar la prueba de recorrido a cada uno de los controles del anexo A de la norma de los Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001:2013 en la entidad Partners Telecom Colombia.

Esta revisión se realizó en un periodo de 3 semanas en donde se calificó cada uno de los requisitos y controles de las normas anteriormente mencionados, arrojando los siguientes resultados

A. Calificación de Requisitos de Seguridad

En la tabla que se muestra a continuación (Tabla 5) se puede observa la calificación obtenida en los requisitos que se encuentran en la norma de Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001:2013, en esta evaluación la empresa obtuvo una calificación de madurez de 1.8 lo que equivale a que la empresa se encuentra en un nivel Ejecutado.

Control	Calificación
R.4 Contexto de la organización	1,80
4.1 Comprensión de la organización y de su contexto	2,00
4.2 Comprensión de las necesidades y expectativas de las partes interesada	1,80
4.3 Determinación del alcance del sistema de gestión de seguridad de la información	1,80
4.4 Sistema de gestión de seguridad de la información	1,80
R.5 Liderazgo	1,80
5.1 Liderazgo y compromiso	1,80
5.2 Política	1,80
5.3 Roles, responsabilidades y autoridades en la organización	1,80
R.6 Planificación	1,80
6.1.1 Consideraciones generales	1,80
6.1.2 Apreciación de riesgos de seguridad de la información	1,80
6.1.3 Tratamiento de los riesgos de seguridad de la información	1,80
6.2 Objetivos de seguridad de la información y planificación para su consecución	1,80
R.7 Soporte	1,80
7.1 Recursos	1,80
7.2 Competencia	1,80
7.3 Concienciación	1,80
7.4 Comunicación	1,80
7.5.1 Consideraciones generales	1,80
7.5.2 Creación y actualización	1,80
7.5.3 Control de la información documentada	1,80
R.8 Operación	1,80
8.1 Planificación y control operacional.	1,80
8.2 Evaluación de riesgos de seguridad de la información.	1,80
8.3 Tratamiento de riesgos de seguridad de la información.	1,80
R.9 Evaluación del desempeño	1,80
9.1 Monitoreo, medición, análisis y evaluación	1,80
9.2 Auditoría interna	1,80
9.3 Revisión por la dirección	1,80
R.10 Mejora	1,80
10.1 No conformidad, acción correctiva	1,80
10.2 Mejora continua	1,80

Tabla 5. Calificación obtenida para los requisitos de la Norma ISO/IEC 27001:2013

En la Figura 5 se puede observar el resultado por cada uno de los requisitos de seguridad de manera gráfica, esto ayuda en la identificación de los requisitos que cuentan con una calificación debajo de la media y de esta manera es más fácil enfocar los esfuerzos a los requisitos que se encuentren con una calificación baja.

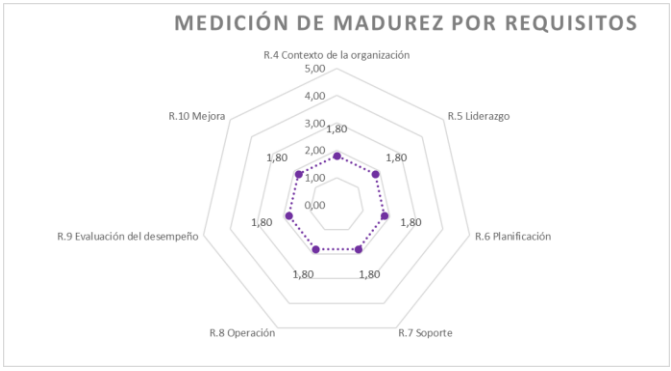

Fig. 7 Resultado de la Calificación Madurez de los Requisitos de Seguridad

B. Calificación de Anexo A de Seguridad

La evaluación de los controles del Anexo de seguridad cumple los mismos principios definidos en el diseño de la herramienta, en la tabla 6 se puede evidenciar la calificación por cada uno de los controles que se encuentran en las 13 familias del Anexo A de la Norma de Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001:2013.

Control	Calificación
A.5 Políticas de seguridad de la información	1,80
A.5.1.1 Políticas para la seguridad de la información	1,80
A.5.1.2 Revisión de las políticas para la seguridad de la información	1,80
A.6 Organización de la seguridad de la información	1,80
A.6.1.1 Roles y responsabilidades en seguridad de la información	1,80
A.6.1.2 Segregación de tareas	1,80
A.6.1.3 Contacto con las autoridades	1,80
A.6.1.4 Contacto con grupos de interés especial	1,80
A.6.1.5 Seguridad de la información en la gestión de proyectos	1,80
A.6.2.1 Política de dispositivos móviles	1,80
A.6.2.2 Teletrabajo	1,80
A.7 Seguridad de los recursos humanos	1,80
A.7.1.1 Investigación de antecedentes	1,80
A.7.1.2 Términos y condiciones del empleo	1,80
A.7.2.1 Responsabilidades de gestión	1,80
A.7.2.2 Concienciación, educación y capacitación en seguridad de la información	1,80
A.7.2.3 Proceso disciplinario	1,80
A.7.3.1 Responsabilidades ante la finalización o cambio	1,80
A.8 Gestión de activos	1,80
A.8.1.1 Inventario de activos	1,80
A.8.1.2 Propiedad de los activos	1,80
A.8.1.3 Uso aceptable de los activos	1,80
A.8.1.4 Devolución de activos	1,80
A.8.2.1 Clasificación de la información	1,80
A.8.2.2 Etiquetado de la información	1,80
A.8.2.3 Manipulado de la información	1,80
A.8.3.1 Gestión de soportes extraíbles	1,80
A.8.3.2 Eliminación de soportes	1,80
A.8.3.3 Soportes físicos en tránsito	1,80
A.9 Control de acceso	1,80
A.9.1.1 Política de control de acceso	1,80
A.9.1.2 Acceso a las redes y a los servicios de red	1,80
A.9.2.1 Registro y baja de usuario	1,80
A.9.2.2 Provisión de acceso de usuario	1,80
A.9.2.3 Gestión de privilegios de acceso	1,80
A.9.2.4 Gestión de la información secreta de autenticación de los usuarios	1,80
A.9.2.5 Revisión de los derechos de acceso de usuario	1,80
A.9.2.6 Retirada o reasignación de los derechos de acceso	1,80
A.9.3.1 Uso de la información secreta de autenticación	1,80
A.9.4.1 Restricción del acceso a la información	1,80
A.9.4.2 Procedimientos seguros de Control inicio de sesión	1,80
A.9.4.3 Sistema de gestión de contraseñas	1,80
A.9.4.4 Uso de utilidades con privilegios del sistema	1,80
A.9.4.4 Uso de utilidades con privilegios del sistema	1,80
A.10 Criptografía	1,80
A.10.1.1 Política de uso de los controles criptográficos	1,80
A.10.1.2 Gestión de claves Control	1,80
A.11 Seguridad física y del entorno	1,80
A.11.1.1 Perímetro de seguridad física	1,80
A.11.1.2 Controles físicos de entrada	1,80
A.11.1.3 Seguridad de oficinas, despachos y recursos	1,80
A.11.1.4 Protección contra las amenazas externas y ambientales	1,80
A.11.1.5 El trabajo en áreas seguras	1,80
A.11.1.6 Áreas de carga y descarga	1,80
A.11.2.1 Emplazamiento y protección de equipos	1,80
A.11.2.2 Instalaciones de suministro	1,80
A.11.2.3 Seguridad del cableado	1,80
A.11.2.4 Mantenimiento de los equipos	1,80
A.11.2.5 Retirada de materiales propiedad de la empresa	1,80
A.11.2.6 Seguridad de los equipos fuera de las instalaciones	1,80
A.11.2.7 Reutilización o eliminación segura de equipos	1,80
A.11.2.8 Equipo de usuario desatendido	1,80
A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia	1,80

Tabla 6 Calificación obtenida en los controles de los 13 dominios del Anexo A de la Norma ISO/IEC 27001;2013 Parte 1.

A.12 Seguridad de las operaciones	1,80
A.12.1.1 Documentación de procedimientos operacionales	1,80
A.12.1.2 Gestión de cambios	1,80
A.12.1.3 Gestión de capacidades	1,80
A.12.1.4 Separación de los recursos de desarrollo, prueba y operación	1,80
A.12.2.1 Controles contra el código malicioso	1,80
A.12.3.1 Copias de seguridad de la información	1,80
A.12.4.1 Registro de eventos	1,80
A.12.4.2 Protección de la información del registro	1,80
A.12.4.3 Registros de administración y operación	1,80
A.12.4.4 Sincronización del reloj	1,80
A.12.5.1 Instalación del software en explotación	1,80
A.12.6.1 Gestión de las vulnerabilidades técnicas	1,80
A.12.6.2 Restricción en la instalación de software	1,80
A.12.7.1 Controles de auditoría de sistemas de información	1,80
A.13 Seguridad de las comunicaciones	1,80
A.13.1.1 Controles de red	1,80
A.13.1.2 Seguridad de los servicios de red	1,80
A.13.1.3 Segregación en redes	1,80
A.13.2.1 Políticas y procedimientos de intercambio de información	1,80
A.13.2.2 Acuerdos de intercambio de información	1,80
A.13.2.3 Mensajería electrónica	1,80
A.13.2.4 Acuerdos de confidencialidad o no revelación	1,80
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	1,20
A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	1,20
A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas	1,20
A.14.1.3 Protección de las transacciones de servicios de aplicaciones	1,20
A.14.2.1 Política de desarrollo seguro	1,20
A.14.2.2 Procedimiento de control de cambios en sistemas	1,20
A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	1,20
A.14.2.4 Restricciones a los cambios en los paquetes de software	1,20
A.14.2.5 Principios de ingeniería de sistemas seguros	1,20
A.14.2.6 Entorno de desarrollo seguro	1,20
A.14.2.7 Externalización del desarrollo de software	1,20
A.14.2.8 Pruebas funcionales de seguridad de sistemas	1,20
A.14.2.9 Pruebas de aceptación de sistemas	1,20
A.14.3.1 Protección de los datos de prueba	1,20
A.15 Relación con proveedores	1,80
A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores	1,80
A.15.1.2 Requisitos de seguridad en contratos con terceros	1,80
A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones Control	1,80
A.15.2.1 Control y revisión de la provisión de servicios del proveedor	1,80
A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor	1,80
A.16 Gestión de incidentes de seguridad de la información	1,80
A.16.1.1 Responsabilidades y procedimientos	1,80
A.16.1.2 Notificación de los eventos de seguridad de la información	1,80
A.16.1.3 Notificación de puntos débiles de la seguridad	1,80
A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	1,80
A.16.1.5 Respuesta a incidentes de seguridad de la información	1,80
A.16.1.6 Aprendizaje de los incidentes de seguridad de la información	1,80
A.16.1.7 Recopilación de evidencias	1,80
A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	1,80
A.17.1.1 Planificación de la continuidad de la seguridad de la información	1,80
A.17.1.2 Implementar la continuidad de la seguridad de la información	1,80
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1,80
A.17.2.1 Disponibilidad de los recursos de tratamiento de la información	1,80
A.18 Cumplimiento	1,80
A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	1,80
A.18.1.2 Derechos de Propiedad Intelectual (DPI)	1,80
A.18.1.3 Protección de los registros de la organización	1,80
A.18.1.4 Protección y privacidad de la información de carácter personal	1,80
A.18.1.5 Regulación de los controles criptográficos	1,80
A.18.2.1 Revisión independiente de la seguridad de la información	1,80
A.18.2.2 Cumplimiento de las políticas y normas de seguridad	1,80
A.18.2.3 Comprobación del cumplimiento técnico	1,80

Tabla 7. Calificación obtenida en los controles de los 13 dominios del Anexo A de la Norma ISO/IEC 27001;2013 Parte 2.

Al concluir de calificar cada uno de los dominios del Anexo A de la Norma de los Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001:2013 se procede a generar las graficas que ayuden a identificar los dominios que se encuentran por debajo de los demás dominios, para la empresa Partners Telecom Colombia el dominio que se encuentra con una calificación inferior es dominio A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información. Esto se puede observar en la Figura 8.

Fig. 8 Resultado de la Calificación Madurez del Anexo A de Seguridad

C. Calificación del Framework de Ciberseguridad NIST SP 800-53.

La calificación de los controles del Framework de Ciberseguridad se extrae de la armonización de los controles del Anexo A y los controles del Framework de la NIST, por esta razón no se realiza una calificación de los controles del Framework por separado, si no que se utiliza la calificación de los requisitos y controles ya calificados y enlaza con los controles de la NIST.

Dominio	Familia	Control	27001	Calificación Control	Calificación Dominio
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	A.8.1.1	1,80	1,81
			A.8.1.2	1,80	
		ID.AM-2: Software platforms and applications within the organization are inventoried	A.8.1.1	1,80	
			A.8.1.2	1,80	
		ID.AM-3: Organizational communication and data flows are mapped	A.13.2.1	1,80	
		ID.AM-4: External information systems are catalogued	A.11.2.6	1,80	
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and	A.8.2.1	1,80	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers,	A.6.1.1	1,80	
		Total ID.AM		**1,80**	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated	A.15.1.3	1,80	
			A.15.2.1	1,80	
			A.15.2.2	1,80	
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	R.4.1	2,00	
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	R.5.1	1,80	
			R.5.2	1,80	
			R.6.2	1,80	
			R.7.4	1,80	
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	A.11.2.2	1,80	
			A.11.2.3	1,80	
			A.12.1.3	1,80	
		ID.BE-5: Resilience requirements to support delivery of critical services are established	A.11.1.4	1,80	
			A.17.1.1	1,80	
			A.17.1.2	1,80	
			A.17.2.1	1,80	
		Total ID.BE		**1,81**	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	A.5.1.1	1,80	
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	A.6.1.1	1,80	
			A.7.2.1	1,80	
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations,	A.18.1.1	1,80	
		ID.GV-4: Governance and risk management processes address cybersecurity risks	R.6.1.1	1,80	
			R.6.1.2	1,80	
			R.6.1.3	1,80	
			R.8.2	1,80	
			R.8.3	1,80	
		Total ID.GV		**1,80**	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	A.12.6.1	1,80	
			A.18.2.3	1,80	
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	A.6.1.4	1,80	
		ID.RA-3: Threats, both internal and external, are identified and documented	R.4.1	2,00	
		ID.RA-4: Potential business impacts and likelihoods are identified	R.6.1.1	1,80	
			R.6.1.2	1,80	
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	A.12.6.1	1,80	
		Total ID.RA		**1,83**	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	R.6.1.1	1,80	
			R.6.1.2	1,80	
			R.6.1.3	1,80	
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	R.6.1.1	1,80	
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific.	R.6.1.1	1,80	
		Total ID.RM		**1,80**	

Tabla 8 Calificación obtenida en los controles del Framework de Ciberseguridad NIST SP 800-53 Rev. 5 Parte 1

OTECT (P	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	A.9.2.1	1,80	1,76
			A.9.2.2	1,80	
			A.9.2.4	1,80	
			A.9.3.1	1,80	
			A.9.4.2	1,80	
			A.9.4.3	1,80	
		PR.AC-2: Physical access to assets is managed and protected	A.11.1.1	1,80	
			A.11.1.2	1,80	
			A.11.1.4	1,80	
			A.11.1.6	1,80	
			A.11.2.3	1,80	
		PR.AC-3: Remote access is managed	A.6.2.2	1,80	
			A.13.1.1	1,80	
			A.13.2.1	1,80	
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	A.6.1.2	1,80	
			A.9.1.2	1,80	
			A.9.2.3	1,80	
			A.9.4.1	1,80	
			A.9.4.4	1,80	
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	A.13.1.1	1,80	
			A.13.1.3	1,80	
			A.13.2.1	1,80	
		Total PR.AC		**1,80**	
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	A.7.2.2	1,80	
		PR.AT-2: Privileged users understand roles & responsibilities	A.6.1.1	1,80	
			A.7.2.2	1,80	
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	A.6.1.1	1,80	
			A.7.2.2	1,80	
		PR.AT-4: Senior executives understand roles & responsibilities	A.6.1.1	1,80	
			A.7.2.2	1,80	
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	A.6.1.1	1,80	
			A.7.2.2	1,80	
		Total PR.AT		**1,80**	
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	A.8.2.3	1,80	
		PR.DS-2: Data-in-transit is protected	A.8.2.3	1,80	
			A.13.1.1	1,80	
			A.13.2.1	1,80	
			A.13.2.3	1,80	
			A.14.1.2	1,20	
			A.14.1.3	1,20	
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	A.8.2.3	1,80	
			A.8.3.1	1,80	
			A.8.3.2	1,80	
			A.8.3.3	1,80	
			A.11.2.7	1,80	
		PR.DS-4: Adequate capacity to ensure availability is maintained	A.12.3.1	1,80	
		PR.DS-5: Protections against data leaks are implemented	A.6.1.2	1,80	
			A.7.1.1	1,80	
			A.7.1.2	1,80	
			A.7.3.1	1,80	
			A.8.2.2	1,80	
			A.8.2.3	1,80	
			A.9.1.1	1,80	
			A.9.1.2	1,80	
			A.9.2.3	1,80	
			A.9.4.1	1,80	
			A.9.4.4	1,80	
			A.9.4.5	1,80	
			A.13.1.3	1,80	
			A.13.2.1	1,80	
			A.13.2.3	1,80	
			A.13.2.4	1,80	
			A.14.1.2	1,20	
			A.14.1.3	1,20	
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	A.12.2.1	1,80	
			A.12.5.1	1,80	
			A.14.1.2	1,20	
			A.14.1.3	1,20	
		PR.DS-7: The development and testing environment(s) are separate from the production environment	A.12.1.4	1,80	
		Total PR.DS		**1,70**	

Tabla 9 Calificación obtenida en los controles del Framework de Ciberseguridad NIST SP 800-53 Rev. 5 Parte 2

Debido a la extensión de controles que se asocian entre la norma de seguridad y el framework de ciberseguridad se requiere fragmentar en varias tablas la información.

Dominio	Familia	Control	27001	Calificación Control	Calificación Dominio
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	A.12.1.2	1,80	1,76025641
			A.12.5.1	1,80	
			A.12.6.2	1,80	
			A.14.2.2	1,20	
			A.14.2.3	1,20	
			A.14.2.4	1,20	
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	A.6.1.5	1,80	
			A.14.1.1	1,20	
			A.14.2.1	1,20	
			A.14.2.5	1,20	
		PR.IP-3: Configuration change control processes are in place	A.12.1.2	1,80	
			A.12.5.1	1,80	
			A.12.6.2	1,80	
			A.14.2.2	1,20	
			A.14.2.3	1,20	
			A.14.2.4	1,20	
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	A.12.3.1	1,80	
			A.17.1.2	1,80	
			A.17.1.3	1,80	
			A.18.1.3	1,80	
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	A.11.1.4	1,80	
			A.11.2.1	1,80	
			A.11.2.2	1,80	
			A.11.2.3	1,80	
		PR.IP-6: Data is destroyed according to policy	A.8.2.3	1,80	
			A.8.3.1	1,80	
			A.8.3.2	1,80	
			A.11.2.7	1,80	
		PR.IP-7: Protection processes are continuously improved	R.10.2	1,80	
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	A.16.1.6	1,80	
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	A.16.1.1	1,80	
			A.17.1.1	1,80	
			A.17.1.2	1,80	
		PR.IP-10: Response and recovery plans are tested	A.17.1.3	1,80	
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	A.7.1.1	1,80	
			A.7.3.1	1,80	
			A.8.1.4	1,80	
		PR.IP-12: A vulnerability management plan is developed and implemented	A.12.6.1	1,80	
			A.18.2.2	1,80	
		Total PR.IP	**1,66**		
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	A.11.1.2	1,80	
			A.11.2.4	1,80	
			A.11.2.5	1,80	
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	A.11.2.4	1,80	
			A.15.1.1	1,80	
			A.15.2.1	1,80	
		Total PR.MA	**1,80**		
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	A.12.4.1	1,80	
			A.12.4.2	1,80	
			A.12.4.3	1,80	
			A.12.4.4	1,80	
			A.12.7.1	1,80	
		PR.PT-2: Removable media is protected and its use restricted according to policy	A.8.2.2	1,80	
			A.8.2.3	1,80	
			A.8.3.1	1,80	
			A.8.3.3	1,80	
			A.11.2.9	1,80	
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	A.9.1.2	1,80	
		PR.PT-4: Communications and control networks are protected	A.13.1.1	1,80	
			A.13.2.1	1,80	
		Total PR.PT	**1,80**		

Tabla 10 Calificación obtenida en los controles del Framework de Ciberseguridad NIST SP 800-53 Rev. 5 Parte 3

Dominio	Familia	Control	27001	Calificación Control	Calificación Dominio
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	A.12.6.2	1,80	1,75
			A.13.1.1	1,80	
			A.13.1.2	1,80	
			A.13.1.3	1,80	
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	A.16.1.1	1,80	
			A.16.1.4	1,80	
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	A.16.1.2	1,80	
		DE.AE-4: Impact of events is determined	A.16.1.4	1,80	
		DE.AE-5: Incident alert thresholds are established	A.16.1.4	1,80	
		Total DE.AE	**1,80**		
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	A.13.1.2	1,80	
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	A.11.1.1	1,80	
			A.11.1.2	1,80	
			A.11.1.3	1,80	
			A.11.1.4	1,80	
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	A.12.4.1	1,80	
		DE.CM-4: Malicious code is detected	A.12.2.1	1,80	
		DE.CM-5: Unauthorized mobile code is detected	A.12.5.1	1,80	
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	A.14.2.7	1,20	
			A.15.2.1	1,80	
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	A.11.2.1	1,80	
			A.12.6.2	1,80	
			A.13.1.2	1,80	
		DE.CM-8: Vulnerability scans are performed	A.12.6.1	1,80	
		Total DE.CM	**1,76**		
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	A.6.1.1	1,80	
		DE.DP-2: Detection activities comply with all applicable requirements	A.18.1.4	1,80	
		DE.DP-3: Detection processes are tested	A.14.2.8	1,20	
		DE.DP-4: Event detection information is communicated to appropriate parties	A.16.1.2	1,80	
		DE.DP-5: Detection processes are continuously improved	A.16.1.6	1,80	
		Total DE.DP	**1,68**		

Tabla 11 Calificación obtenida en los controles del Framework de Ciberseguridad NIST SP 800-53 Rev. 5 Parte 4

Dominio	Familia	Control	27001	Calificación Control	Calificación Dominio
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	A.16.1.5	1,80	1,80
		Total RS.RP	**1,80**		
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed	A.6.1.1	1,80	
			A.16.1.1	1,80	
		RS.CO-2: Events are reported consistent with established criteria	A.6.1.3	1,80	
			A.16.1.2	1,80	
		RS.CO-3: Information is shared consistent with response plans	A.16.1.2	1,80	
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	R.9.3	1,80	
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational	R.7.4	1,80	
		Total RS.CO	**1,80**		
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	A.12.4.1	1,80	
			A.12.4.3	1,80	
			A.16.1.5	1,80	
		RS.AN-2: The impact of the incident is understood	A.16.1.6	1,80	
		RS.AN-3: Forensics are performed	A.16.1.7	1,80	
		RS.AN-4: Incidents are categorized consistent with response plans	A.16.1.4	1,80	
		Total RS.AN	**1,80**		
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained	A.16.1.5	1,80	
		RS.MI-2: Incidents are mitigated	A.12.2.1	1,80	
			A.16.1.5	1,80	
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	A.12.6.1	1,80	
		Total RS.MI	**1,80**		
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	A.16.1.6	1,80	
		RS.IM-2: Response strategies are updated	A.16.1.6	1,80	
		Total RS.IM	**1,80**		
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	A.16.1.5	1,80	1,80
		Total RC.RP	**1,80**		
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	A.16.1.6	1,80	
		RC.IM-2: Recovery strategies are updated	A.16.1.5	1,80	
		Total RC.IM	**1,80**		
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	R.7.4	1,80	
			A.6.1.3	1,80	
			A.6.1.4	1,80	
		RC.CO-2: Reputation after an event is repaired	R.7.4	1,80	
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	R.7.4	1,80	
			A.6.1.5	1,80	
		Total RC.CO	**1,80**		

Tabla 12 Calificación obtenida en los controles del Framework de Ciberseguridad NIST SP 800-53 Rev. 5 Parte 5

Después de identificar el valor promedio de los controles del Anexo A que hacen match con lo controles del Framework de Ciberseguridad de la NIST, de realizan las graficas correspondientes

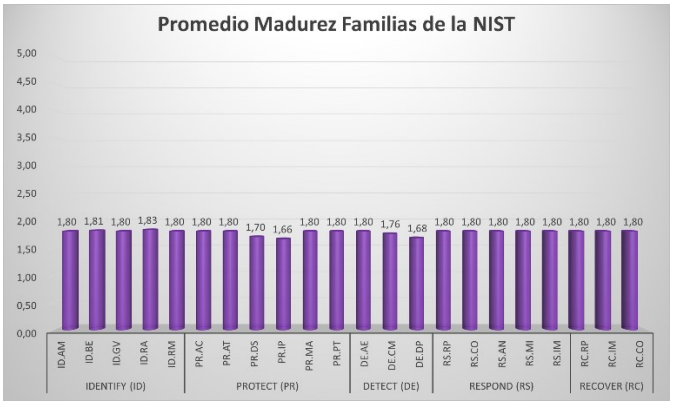

Fig. 9. Resultado de la Calificación Madurez de los controles del Framework de Ciberseguridad NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

En la Figura 9 se evidencia el resultado por familias de controles y por los controles que están contenidos en las familias.

El resultado de madurez para esta calificación se pueden identificar otros controles y/o vértices que cuentan con niveles inferiores de seguridad.

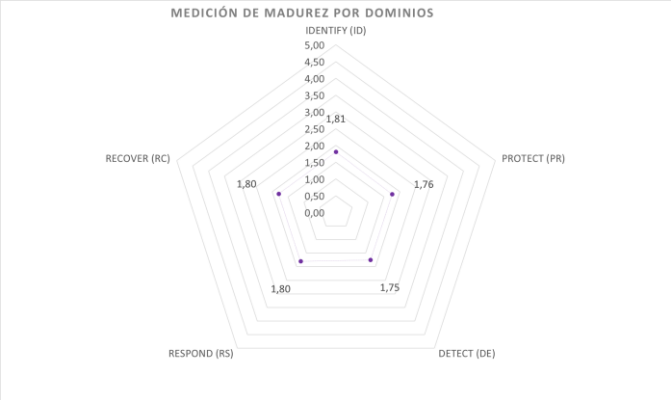

Fig. 10. Resultado de la Calificación Madurez de las familias del Framework de Ciberseguridad NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

En la Figura 10 se evidencian en muy alto nivel las calificaciones de las familias de controles del Framework de la Nist SP 800-53, esto implica que se debe realizar un trabajo focalizado a la familia de Detectar y Proteger, esto con el fin de contar con un sistema de Seguridad y Ciberseguridad uniforme.

D. Recomendaciones para mejorar la madurez del Sistema de Seguridad y Ciberseguridad.

Para mejorar la Seguridad de la Información y Ciberseguridad, se recomienda mantener una mejora continua de sistema. Para esto se recomienda seguir las siguientes recomendaciones.

Nivel de madurez Ejecutado se encuentra en una calificación mayor a 1 y menor a 2, se debe ser ejecutado el control, y debe estar divulgado con las partes interesadas al interior y exterior de la compañía, el proceso de divulgación se debe realizar mínimo una vez al año o cuando se genere un cambio importante en las políticas de la empresa.

Nivel de madurez Gestionado: Para alcanzar este nivel de Gestionado la calificación debe ser igual a 2, para poder conseguir esta calificación se recomienda evaluar la documentación evaluada, para esto se deben utilizar herramientas que ayuden en la medición y almacenamiento de los resultados, ya se estos son evidencia de la divulgación y entendimiento del tema.

Si los resultados no son los esperados se recomienda utilizar métodos diferentes de socialización y culturización, para que los funcionarios apliquen las políticas de la compañía.

Nivel de madurez Establecido, para obtener este nivel de madurez, se recomienda realizar una prueba de recorrido a los controles, esto quiere decir que se debe realizar un proceso formal de auditoría que abarque todos los requerimientos y controles de la norma de gestión de Seguridad de la Información.

Para aumentar el nivel de madurez superior a 3 se debe realizar un monitoreo en cada uno de los controles, que ayuden a identificar las desviaciones de las actividades que se realizan y poder realizar la mejora continua del sistema.

Después de implementar un monitoreo se recomienda definir e implementar indicadores de gestión que ayuden a apalancar la medición del sistema de gestión, después de la definición, implementación y gestión de las desviaciones de los indicadores y evidencias de los ajustes y mejoras se puede considerar que la compañía se encuentra en un nivel de madurez predecible o su calificación es mayor a 4.

Para aumentar el nivel de madurez se debe invertir en herramientas que ayuden a automatizar los controles de seguridad de seguridad de la información, esto con el fin de evitar el error humano. Cuando la organización logre optimizar los controles de la norma, se puede pensar en un nivel de madurez Optimizado.

VII. CONCLUSIONES

Mediante el desarrollo de la herramienta de armonización de los controles de la norma ISO/IEC NTC 27001:2013 Sistema de Gestión de Seguridad de la Información y framework de ciberseguridad SP NIST 800-53 Security and Privacy Controls for Information Systems and Organizations, y la evaluación de seguridad realizada en la empresa PTC, se puede evidenciar que la calificación y nivel de madurez es muy similar para la los requisitos, controles del Anexo de la norma ISO 27001 y el framework de ciberseguridad de la NIST SP 800-53.

El proyecto se enfocó en el diseño y desarrollo de la herramienta de armonización de los controles de la ISO 27001:2013 y la NIST SP800-53 v5, y posterior prueba de la herramienta. Para el diseño de la herramienta se realiza un levantamiento de información referente a herramientas que

realicen una medición de madurez del sistema de gestión, frameworks de medición y evaluación de procesos, adicional a esto se realiza el levantamiento de información al respecto de la correlación e integración de las normas de Seguridad de la información y Ciberseguridad tendencia en el mercado.

Una vez finalizado el levantamiento de información referente a las herramientas de medición de madurez, se evidencia que se cuenta con un amplio escenario de investigación, ya que solo se identificó que la única organización que está trabajando en este tipo de herramientas es el Ministerio de Tecnologías de la Información y Comunicaciones, la cual está enfocada para las organizaciones gubernamentales.

Después de probar la herramienta, se procede a realizar mejoras a la medición y cálculo del nivel de madurez, al terminar con estos ajustes en la medición, se generan unas recomendaciones para mejorar el nivel de madurez de la compañía.

Al terminar el proceso de evaluación en PTC se determina que el área idónea para tener el control actualización y/o modificación de la herramienta de medición de la madurez, es Seguridad de la Información, sin embargo, se plantea entregar una versión al área de auditoría, esto con el fin de unificar los procesos de revisión y evaluación de la compañía y al ser un área independiente en la organización.

REFERENCES

[1] ALARCON Dora Mayerli y HERRERA Angie Katerine. Revisión del estándar de seguridad ISO /IEC 30141 como arquitectura de referencia para IoT. Bogotá D.C.: Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información.

[2] ALMAGRO Luis, "MARCO NIST CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad". Internet (https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf)

[3] ANGARITA Cristian y GUZMÁN Camilo. Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá. Bogotá D.C.: Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información.

[4] ARCILA Luis Eduardo. Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de Seguridad de la Información. Bogotá D.C.: Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. 2019

[5] Banco Interamericano de Desarrollo. Reporte Ciberseguridad 2020: CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE.

[6] Documento CONPES 3701 Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación, Lineamientos de Política para Ciberseguridad y Ciberdefensa. Bogotá D.C.: 2011

[7] Documento CONPES 3854 Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación, Política Nacional de Seguridad Digital. Bogotá D.C.: 2011

[8] Documento CONPES 3995 Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación, Política Nacional de Confianza y Seguridad Digital. Bogotá D.C.: 2011

[9] ESTADOS UNIDOS. CIS Center for internet Security. CIS Critical Security Controls v8 Washington, DC, 2021

[10] ESTADOS UNIDOS. Cloud Security Alliance CSA. Cloud Controls Matrix and CAIQ v4, 2021

[11] FRANCIA. Organización International de Policía Criminal INTERPOL. Ciberseguridad Efectos de la Covid-19 (agosto, 2020) Lyon, 2020

[12] COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. Resolución 500 de 2021 (10, marzo, 2021). Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

[13] CRISTIANO Juan Pablo. Implementación de defensa en profundidad en empresa Pyme. Bogotá D.C.: Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información.

[14] GONZÁLEZ Rony Mitshiu y COLO José Humberto. Diseñar un modelo para implementar un sistema de gestión de Seguridad de la Información para una PYME del sector privado. Bogotá D.C.: Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información.

[15] GUZMAN Sandra Liliana, Guía para la implementación de la norma ISO 27032. Bogotá D.C.: Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información.

[16] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION, Sistema de gestión de Seguridad de la Información. NTC ISO/IEC 27001. Bogotá D.C.: El instituto, 2013.

[17] ISACA. Marco de Referencia COBIT 2019: Objetivos de gobierno y gestión. Bogotá D.C: 2019. 20 p ISBN 978-1-60420-790-3

[18] ISACA. Marco de Referencia COBIT5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Estados Unidos: 2012. 41 p ISBN 978-1-60420-282-3

[19] MARTINEZ Fabio. Plan de concienciación sobre la importancia de la Seguridad de la Información en las entidades de salud del sector público de Bogotá. Bogotá D.C.: Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información.

[20] MATIZ Juan Carlos y RUEDA Miguel Arturo. Diseño de un modelo de seguridad y privacidad de la información para las empresas de empleo temporal basado en la norma ISO 27001. Bogotá D.C.: Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información.

[21] MORGAN Steve, 2019 Annual Official Cybersecurity Ventures Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades, Estados Unidos: 2019.

[22] National Institute of Standars and Technology, Security and Privacy Controls for Informaation Systems and Organizations NIST Special Publication 800-53 Revision 5. Estados Unidos: 2020

[23] Pmg-ssi, ISO 27001: El modelo de madurez de la seguridad de la información. Internet (https://www.pmg-ssi.com/2015/02/iso-27001-el-modelo-de-madurez-de-la-seguridad-de-la-informacion/)

[24] Semana, ¿Quién es Julian Assange, el fundador de Wikileaks?. Internet (https://www.semana.com/mundo/articulo/quien-julian-assange-fundador-wikileaks/125225-3/.)

[25] TRENDMICRO, Attacks From All Angles 2021 Midyear Cybersecurity Report. Internet (https://www.trendmicro.com/vinfo/fr/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup)

[26] ZÁRATE Iván Javier, Diagnóstico de riesgos y vulnerabilidades en Seguridad de la Información a la infraestructura tecnológica de la empresa 4s ingeniería sas, con el objetivo de generar una política de seguridad. Bogotá D.C.: Universidad Central. Facultad de ingeniería. Departamento de Ingeniería de Sistemas, 2017

Iván Javier Zárate Santos. Ingeniero de Sistemas en la Universidad Central, Especialista de seguridad Informática en WOM, con certificaciones de Auditor interno ISO/IEC 27001:2013, Automated Mobile Application Security Assessment, Certified Offensive and Defensive Security Professional