TRABAJO DE GRADO

GUíA PARA EL ABORDAJE DE LA NORMA ISO 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD.

AGUSTÍN RODRÍGUEZ SUÁREZ - COD: 63000225

FABIO ALEXANDER ROJAS RUIZ – COD: 63000211

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2022

TRABAJO DE GRADO

GUíA PARA EL ABORDAJE DE LA NORMA ISO 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD.

AGUSTÍN RODRÍGUEZ SUÁREZ - COD: 63000225

FABIO ALEXANDER ROJAS RUIZ – COD: 63000211

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Docente

SANDRA MILENA BERNATE BAUTISTA
Ingeniero de sistemas

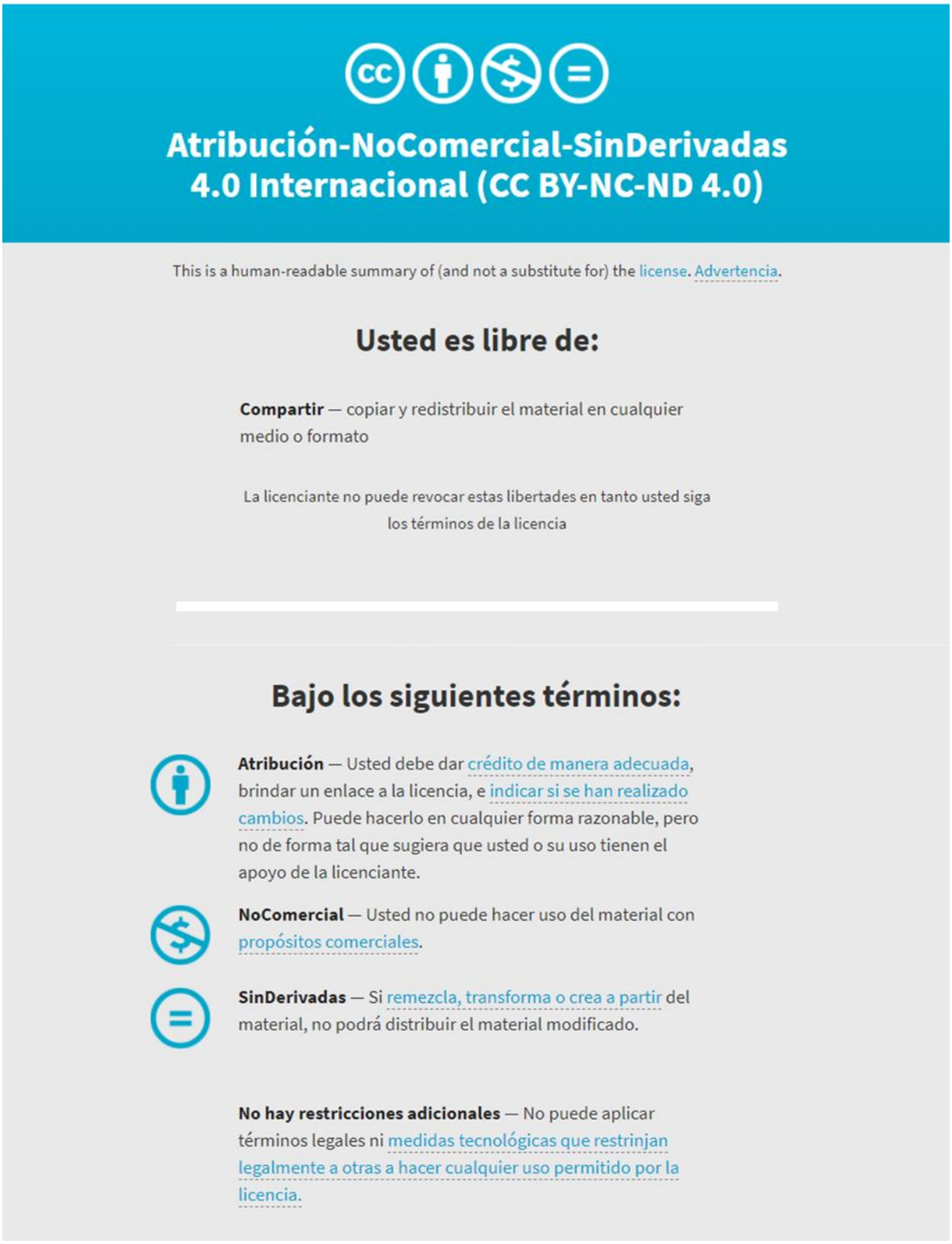
UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2022



https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Tecnologías emergentes como la computación en la nube, Big data y IoT (Internet of Things) son solo algunos ejemplos de infinitas posibilidades de comunicación, han permitido administrar empresas sin salir de casa; sin duda alguna, una razón lo suficientemente valiosa para que las empresas tengan presencia en el ciberespacio; ya sea para vender, comprar, chatear con clientes, hacer el inventario de bienes, incluso con la intención de ganar reputación, las empresas han encontrado en internet las razones suficientes para asumir los riesgos inherentes que trae consigo la implementación y su uso.

Estos riesgos toman valor cuando las empresas en su afán de implementar ciertas tecnologías recurren al ciberespacio sin la conciencia suficiente de los riesgos a los que se expone, sin evaluar sus vulnerabilidades y sin los controles de seguridad necesarios; no obstante, los ciberataques siguen creciendo como si se tratara de una infección viral.

Muchas empresas han centrado sus esfuerzos en crear documentos, políticas, procesos, procedimientos y herramientas para dar frente a los ciberataques, a este conjunto de elementos también se les conoce como marcos de ciberseguridad, y han facilitado a las de empresas las actividades para combatir este fenómeno digital, sin embargo, muchos marcos de ciberseguridad se han creado en el mundo con múltiples definiciones, estructuras e interpretaciones,

La norma ISO/IEC 27110:2021 es el resultado de los esfuerzos de la ISO para garantizar que se utilice el conjunto mínimo de conceptos en la definición de marcos de ciberseguridad, aliviando la carga a los creadores de marcos y en si, con el objetivo de que estos sean flexibles con otras normas e implementaciones ya realizadas de la organización, así como interoperable y compatible con otros marcos.

Entre otros principios y objetivos de la norma, está la capacidad de ser aplicada a cualquier organización, no importa el tamaño, la naturaleza o el tipo, pues posee los conceptos necesarios para organizar un marco de ciberseguridad que responda de forma correcta y coherente a las necesidades del contexto; es por esto que **LA GUÍA PARA EL ABORDAJE ISO/IEC 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD,** desarrolla una interpretación simple, comprensible a todas las partes interesadas, didacta para una mejor apropiación de la norma y dirigida a creadores de marcos de todo tipo de empresas.

En la presente guía se describen los conceptos necesarios para la creación de marcos de ciberseguridad con una visión sencilla sobre sus especificaciones; su contenido trae consigo recomendaciones sobre las categorías a implementar, el diseño que puede ser usado y ejemplos prácticos que referencian las normas ISO/IEC que prevén las directrices necesarias para su estructura según el contexto de la organización.

1. GENERALIDADES

1.1 LÍNEA DE INVESTIGACIÓN

GEGI - Gestión Empresarial y Gestión de Innovación

“Plan de trabajo: Fortalecer la producción investigativa en entornos de estrategia, creatividad e innovación para tomar decisiones sistémicas asertivas en las áreas funcionales y tecnológicas de las organización en los sectores social, económico, industrial, tecnológico, de salud y de prestación de servicios con el uso y apropiación de las tecnologías de la información y las comunicaciones, para generar conocimiento y desarrollo tecnológico innovativo, a partir de investigaciones que redunden en el uso de mejores prácticas, aplicación de escenarios, usando metodologías o modelos de gestión, de acuerdo con las necesidades y problemas del entorno de competencia en el que se desenvuelven las organizaciones. (...)”

1.2 PLANTEAMIENTO DEL PROBLEMA

El mundo entero busca estar seguro en el ciberespacio, que toda la información que se comparte sea protegida sin importar el tamaño o el valor que tenga, ya que estar expuestos a delitos informáticos, es el riesgo que asumimos por consumir servicios tan básicos como enviar un mensaje de texto, publicar una foto en redes sociales o incluso, hacer una llamada. Con el paso del tiempo ha surgido una nueva era de tecnología con una transformación digital para el mundo, que consigo trajo nuevos retos para las compañías los cuales nos hacen tener una modificación e implementación en los procesos tecnológicos, que a su vez contrae riesgos de seguridad y ciberseguridad con un gran impacto en los diferentes sectores financieros, social, ambiental, agropecuario, educativo, etc. por lo cual nos exponemos a riesgos como el secuestro o robo de información, a la propiedad intelectual, sabotaje e interrupción de los servicios.

Con el constante cambio que tenemos en las nuevas tecnologías tales como computación en la nube, el internet de las cosas, big data - analítica, y blockchain, que representan riesgos en materia de ciberseguridad para las compañías, debido a que el pirata informático se encuentra explorando de manera continua como atacar a través de ingeniería social, phising, malware, virus e inclusión por puertas trasera.

.

El sector económico, especialmente el terciario quien por su actividad económica, hace uso del ciberespacio como medio para la interacción con los clientes, consumiendo servicios en los que prevalece el atractivo publicitario y las personas suelen dejar datos con mayor frecuencia; información que las empresas en su buen uso, y entre otras cosas, destina a la creación de algoritmos de predicción, segmentación de campañas publicitarias o como objetivo de difusión, sin embargo,

en cualquiera de estos escenarios y de forma bilateral, la información pierde control de dominio por parte de su propietario.

Aunque su actividad económica se basa en servicios y es precisamente la necesidad de ofrecerlos al cliente objetivo quien lo hace especial consumidor del ciber espacio, no podemos dejar de lado las empresas que por su actividad económica están clasificados como sector secundario (destinadas a la industria) y las empresas del sector primario dedicadas a las agricultura; a hoy, y con la certeza de que crecerá la producción de máquinas y elementos que buscan mejorar la productividad en las actividades de este sector, se han diseñado múltiples dispositivos conectados a internet, que permite entre muchas y otras cosas, a la administración y el monitoreo.

De su parte, en estos sectores podemos clasificar aquellas empresas que por su actividad económica provee a las personas servicios como las comunicaciones, alimentación, transporte, fabricación de tecnologías de la información, salud, suministro de agua, incluso, servicios de emergencia; con la necesidad de no tener intrusos informáticos que cambien, detengan o dañen el correcto funcionamiento de sus dispositivos de fabricación, y de igual importancia, otra información de la empresa capaz de alterar el correcto funcionamiento de procesos o procedimientos.

En este panorama, el ciberespacio trae consigo aparentemente en igual proporción, beneficios y riesgos, una situación difícil de manejar, con tantas personas del lado bueno como del lado criminal, con respaldo de importantes organizaciones y con grandes investigaciones que dejan a su paso técnicas, métodos, documentación y procedimientos como apoyo a la ciberseguridad, con la clara certeza que no todo está en conocimiento y se sigue trabajando para enfrentar con mayor tranquilidad esta época de cambios tecnológicos.

Tecnologías emergentes son creadas con el propósito de suplir necesidades comunes del mundo, muchas de estas fueron desarrolladas años atrás; sin embargo, en nuestro país y especialmente en Latinoamérica, en donde nos recuperamos del desarrollo fallido y un evidente fracaso de modernización a causa del desbalance económico, político y social en las décadas de los 60’s y 80’s, no eran accesibles o simplemente las desconocemos.

Internet de las cosas o Internet of Things (IoT), por ejemplo, es tan increíble como inseguro, una tecnología muy accesible a las personas, deseada y con gran aceptación, incluida en las necesidades cotidianas, con IoT se podría prender el horno u otro elemento de la cocina mediante WiFi, monitorizar y controlar las luces de los semáforos de una ciudad, incluso, podría encargarse del total funcionamiento de plantas industriales; y así, con estos y otros beneficios también existe el riesgo de que un cibercriminal prenda fuego al horno e inicie un incendio, altere el tráfico de una ciudad ocasionando accidentes de tráfico o deje sin servicios básicos como agua o energía eléctrica a una población, pues la información que permite su

funcionamiento, una vez relacionada con internet queda vulnerable a intrusos.

De igual manera otra tecnología que ha brindado a las empresas beneficios importantes, especialmente en el procesamiento de datos ha sido la computación en la nube, aunque permitió el reemplazo de centros de datos físicos por servidores web mejorando el rendimiento y reduciendo costos de mantenimiento, agregó riesgos de administración para la información contenida.

El BlockChain por su parte, es una tecnología que está tomando fuerza y aceptabilidad por parte de los ciber usuarios, y con ello, se suman riesgos para las empresas y las personas, el BlockChain consiste en la verificación colectiva de computadores que verifican las transacciones para garantizar la integridad, esto sin duda genera confianza, pero también representa un blanco para ciberdelincuentes.

Otra tecnología importante de mencionar, que favorece a las empresas en la transformación de grandes cantidades de información en conocimiento, es Big Data, con esta tecnología las empresas han logrado tomar decisiones a partir del análisis de los datos, la construcción de algoritmos de predicción y segmentación de clientes para el mejoramiento en la experiencia del usuario.

Existen leyes nacionales como la 1273-2009 y la 1581-2012 que clasifican, tipifican y regula el uso de la información personal obtenida en las empresas y así mismo otorga derecho de olvido a las personas, acuerdos internacionales para capturar ciber atacantes sin importar su ubicación geográfica, directrices, estándares y documentación respaldada por importantes centros de investigación; aun así, la seguridad en las empresas consiste de un ejercicio mancomunado de todo el personal que la compone, del reconocimiento de sus activos así como del uso apropiado de las tecnologías y recursos a disposición.

1.2.1 ANTECEDENTES DEL PROBLEMA

Muchos esfuerzos se han aunado para el desarrollo de la ciberdefensa; desde el 2013 el mundo tiene a su disposición la norma ISO/IEC 27001:2013 con la cual podemos gestionar los riesgos de seguridad de la información, esta norma en complemento con la ISO/IEC 27002:2013, actualizada en el 2022, proporcionaba los controles que permiten dar frente a estos riesgos, sin embargo, faltaba cubrir otros aspectos importantes de la seguridad en el ciberespacio, específicamente abarcar controles para contenedores de la información, las personas y la infraestructura crítica.

En el 2014 el Instituto Nacional de Estándares y Tecnología de los EE.UU. bajo una orden presidencial diseñaron un marco de ciberseguridad que permitía abordar temas de la ciberseguridad que no estaban contemplados previamente; el marco NIST está compuesto por una estructura referencial de buenas prácticas que permite a las organizaciones definir y centralizar sus esfuerzos en la ciberdefensa,

de manera tal, que pueda administrar todos los activos que hagan parte del ecosistema tecnológico.

El 2012, la Organización Internacional de Normalización publicó la ISO/IEC 27032:2012 con el fin de aliviar vacíos respecto a los controles de seguridad de la información y su uso en el ciberespacio, así como aspectos de contenedores de la misma; ISO/IEC 27032:2012 “Directrices para la ciberseguridad” es hasta entonces la primera norma ISO que abarca el concepto de ciberespacio.

En el 2020, la Organización Internacional de Normalización, publica la norma ISO/IEC 27100:2020 quien aborda la ciberseguridad de manera conceptual, estableciendo los requisitos mínimos para la ciberdefensa, siendo flexible y aclarando que es aplicable a todo tipo de empresa sin importar su tipo, tamaño o naturaleza, incluso, detalla las diferencias que existen entre seguridad de la información y el ciberespacio, no obstante, las tecnologías emergentes y los nuevos riesgos conocidos, han llevado a pensar que los riesgos no son solo un problema de la información o de los contenedores físicos, ni operacional ni ejecutivo, sino, que se trata de un problema organizacional, que no afecta los recursos únicamente, viendo la necesidad de proteger a las empresas y a las personas que hace parte de ella.

Es así como en el 2021, se publicó la ISO/IEC TS 27110:2022, cerrando brechas respecto al manejo de la seguridad en el ciberespacio, proporcionando una visión flexible, con conceptos ya conocidos en otros marcos populares de ciberseguridad, con el propósito de hacerlo interoperable, aliviando cargas de trabajo a los creadores de marcos de ciberseguridad.

1.2.2 Pregunta de investigación

¿Cómo abordar la norma ISO/IEC 27110:2021 para la implementación de marcos de ciberseguridad en las empresas?

1.3 Justificación

Los múltiples beneficios tecnológicos que acaparan las empresas se relacionan con presencia en el ciber espacio: la interacción con clientes en red, las ventas, el cumplimiento de objetivos misionales o incluso por reputación, estos son solo algunos de los factores que motivan a las organizaciones a implementar apresuradamente tecnologías interconectadas, en algunos casos sin el nivel de conciencia suficiente que permita afrontar las amenazas a las que se expone.

Las ciber amenazas son en gran medida variables y probablemente dependientes de factores que no se identifican hasta la evaluación de riesgos, situación que permite deducir que estos no emergen a partir de la conciencia sobre la ciberseguridad, sino que surgen desde el momento en el que las organizaciones se

relacionan con el ciber espacio, y en consideración a ello, es importante que todas las empresas conozcan y desplieguen marcos de ciberseguridad que permitan reunir buenas prácticas y controles tanto para la identificación de los riesgos, como para la definición de planes que permitan dar frente de forma ordenada y coherente a los mismos, todo esto, conforme a los objetivos de la organización, los requisitos de las partes interesadas y las necesidades del contexto en general.

Suele asociarse los marcos de ciberseguridad a grandes empresas, especialmente por su naturaleza: bien sea por infraestructura crítica o por grandes almacenes de datos, sin embargo, por más mínimo que sea el porcentaje de relación con internet, todas las empresas sin importar su tipo, tamaño o naturaleza están expuestas a las amenazas allí contenidas, y es por esto que la definición de controles y buenas prácticas, aportan valor a la protección de sus activos, las personas y la organización.

La GUÍA PARA EL ABORDAJE ISO/IEC 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD está diseñada para que los creadores de marcos de ciberseguridad aborden de una manera fácil el contenido de la norma ISO/IEC 27110:2021 como alternativa para la definición de marcos de ciberseguridad en las empresas basado en estándares de la Organización Internacional de Estandarización, buscando facilitar mediante el lenguaje sencillo, el análisis y la comprensión de los conceptos necesarios para hacer del marco resultante, una estructura flexible, compatible e interoperable.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Apoyar a los creadores de marcos de ciberseguridad de cualquier organización mediante una guía publicada en internet para el abordaje de la norma ISO/IEC 27110:2021 que sea comprensible a todas las partes interesadas.

1.4.2 OBJETIVOS ESPECÍFICOS

- Identificar referencias a controles y buenas prácticas, caracterizando su naturaleza con base a los conceptos para la definición de marcos de ciberseguridad basados en la norma ISO/IEC 27110:2021.
- Desarrollar una estrategia que permita a los creadores de marcos de ciberseguridad de cualquier organización interpretar fácilmente la norma ISO/IEC 27110:2021
- Aplicar lenguaje sencillo que permita el entendimiento de todas las partes interesadas.

2 MARCO DE REFERENCIA

El Sistema de Gestión de Seguridad de la Información (SGSI) soportada en la norma ISO 27001:2005 busca garantizar la selección de controles de seguridad adecuados, permitiendo a las empresas la gobernanza, protección y gestión de sus activos de información.

Un ataque digital hace referencia a cualquier evento mal intencionado por medios digitales, que pueden materializar un incidente de seguridad viendo afectada la integridad, confidencialidad y disponibilidad de la información.

Por lo anterior, la ciberseguridad se ha convertido en uno de los retos de mayor importancia en las empresas; se diseñan políticas y se aplican estándares de seguridad en buscan reducir los riesgos de ataque, implementando mecanismos que, a su vez, reduzcan las vulnerabilidades existentes.

Es así como las empresas, con base a los principios de flexibilidad, compatibilidad y operabilidad; sin importar su tamaño, tipo o naturaleza pueden crear marcos de ciberseguridad, actividad que consiste en reunir un conjunto de normas, estándares y buenas prácticas para administrar de forma oportuna y eficaz los riesgos de ciberseguridad.

Con el fin de facilitar su creación y aplicabilidad, la Organización Internacional de Normalización (ISO), en conjunto con profesionales de todo el mundo, recolecta y estandariza las mejores prácticas utilizadas, permitiendo, además, la identificación y comprensión de los conceptos necesarios para la gestión de ciberataques.

Dicha estandarización, publicada como norma ISO/IEC 27110:2021, cuenta con una estructura organizada basada en High level Structure (HLS) que facilita la implementación, el contenido y el enfoque de un marco de ciberseguridad confiable.

¿Por qué se hace importante implementar un marco de ciberseguridad?, Las nuevas tecnologías brindan oportunidades de crecimiento y mejoramiento a las empresas conectadas en el ciberespacio, pues sin duda alguna, se suplen necesidades respecto a la oferta y la demanda, la reputación, fidelización entre otras, beneficios que conllevan a la adopción, sin embargo, algunos factores inherentes a su implementación agregan vulnerabilidades, pues en el ciberespacio podrían existir riesgos no conocidos y por ende ninguna metodología de protección; entre los factores de riesgo más comunes esta:

- Adopción acelerada y desordenada de tecnologías emergentes: Es de esperarse que la transformación digital en las empresas tome valor exponencial día a día, sin embargo, la falta de planeación, principalmente en la detección de posibles amenazas y definición de controles, aumenta la probabilidad de riesgo.

- Incremento en las transacciones electrónicas: Otro factor importante para tener en cuenta para el análisis de los riesgos está representado por la cantidad de transacciones electrónicas que se realice, como capturar información de clientes, pagos en línea, ventas, compras etc. teniendo como premisa que, a mayor flujo de transacciones, mayor es la exposición al riesgo.

- Canales inseguros: Conectarnos a internet lo ha sido todo, muchos procesos manuales han sido automatizados y podemos ejecutarlos desde casa o cualquier lugar conectado a internet, pero es justamente esto un factor de riesgo: la educación virtual, el teletrabajo e incluso la telemedicina; el intercambio constante de información y la necesidad de comunicación conllevan a las conexiones por redes no seguras, a entablar transferencia de información por canales desconocidos, redes no protegidas y redes intervenidas.

Los marcos de ciberseguridad reúnen de forma organizada y estructurada todos los esfuerzos de la organización tales como actividades, herramientas, documentos e implementaciones previas para abordar la ciberseguridad.

3 METODOLOGÍA

3.1 FASES DEL TRABAJO DE GRADO

3.1.1 FASE 1: ANÁLISIS

Los avances relacionados a la tecnología han sido bien aceptados en la sociedad por sus evidentes beneficios, las empresas, por ejemplo, reconocen que su presencia en el ciberespacio agrega valor a su misión institucional sin importar la naturaleza de sus objetivos, pues bien, se sabe que en internet podemos encontrar todo tipo de bienes y servicios.

Desde el nacimiento de la conexiones de red se ha pensado en los múltiples riesgos inherentes a ello, y con ello, leyes alrededor del mundo que buscan proteger a las personas en aspectos de identidad y adulterios; el convenio de Budapest por ejemplo, que entró en vigor el 01 de julio de 2014, propende la armonización de leyes entre naciones y de esta manera castigar sin fronteras los delitos informáticos, aquí mismo en Colombia, leyes para la protección de datos como la 1266 del 2008, la 1273 del 2009 y la 1581 2012 emergieron a partir de la necesidad de establecer lineamientos constitucionales para la administración y protección de la información suministrada por el titular de la misma.

La Organización Internacional de Estandarización, conocida como ISO por sus siglas en inglés (International Organization for Standardization) publicó en el 2009 la primera version del estandar ISO/IEC 27000: “Information technology — Security techniques — Information security management systems — Overview and vocabulary”, posteriormente actualizado en el 2012, 2014, 2016 y 2018, esta norma ofrece una descripción general de los sistemas de gestión de seguridad de la información, así como los términos que se deben interpretar y usar.

ISO/IEC 27001:2013 es la segunda versión de esta ISO, la primera fue en el 2005 y esta norma detalla los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información, todo esto, mediante un conjunto estructurado de controles también denominado SGSI (Sistema de Gestión de Seguridad de la Información), que, a su vez, es un marco donde las empresas identifican, evalúan y tratan los riesgos de la información.

Uno de los principales aportes a la ciberseguridad que ha dado la ISO, fue la publicación de la ISO/IEC 27002, un estándar internacional popular que describe una selección genérica de controles de seguridad de la información, se podría decir que el objetivo de esta norma es la de proporcionar controles con el fin de que las organizaciones seleccione y aplique según corresponda al contexto de la empresa, aquellos que se consideren indispensables para la mitigación de riesgos de seguridad de la información.

Y así, a la familia ISO/IEC 27000 se unieron normas como la ISO/IEC 27003, ISO/IEC 27004 y ISO/IEC 27005 las cuales fortalecen los conceptos, requerimientos y aporta aclaraciones sobre las buenas prácticas en la implementación, medición y monitoreo del SGSI, así como para a gestión de riesgos de seguridad de la información, sin embargo, llama la atención que solo hasta la publicación de la norma ISO 27017 la Organización Internacional de Normalización aborda el tema de contenedores físicos de la información, específicamente esta norma está relacionada con computación en la nube, abriendo múltiples brechas de interpretación, pues se hace necesario complementar los controles de la ISO/IEC 27002:2013 que permitan gestionar de forma adecuada y pertinente las actividades de los clientes y proveedores de servicios de nube.

Pero entonces, ¿seguridad de la información o ciberseguridad?; a este tipo de interrogantes se sumó la necesidad de identificar los alcances de las normas técnicas con relación a las personas que proveen y/o administran la información y la presencia de las empresas en el ciberespacio, sin dejar de lado la protección a los contenedores físicos de la misma, actividades alentadas por la necesidad proteger la infraestructura crítica de ciberataques, por mencionar una de las razones importantes de abordar la seguridad de la información desde el amplio espectro del ciberespacio.

Para resolver estas dudas se publicó en el 2012 la norma ISO/IEC 27032:2012, donde oficialmente se aborda la ciberseguridad definida como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, y a su vez, el ciberespacio como un entorno complejo que resulta de la interacción de personas, software y servicios en internet por medio de dispositivos tecnológicos y redes conectadas, su estructura y contenido registra temas como activos en el ciberespacio, roles de las partes interesadas en la ciberseguridad y un marco de intercambio de información y coordinación, y aunque se emergen con ella controles de seguridad en la red, es preciso mencionar que tal como se define el ciberespacio, destacado como un entorno complejo, lo hace altamente variable en riesgos y amenazas.

Así las cosas, se podría decir que la ISO/IEC 27032:2012, es una adaptación de la definición de seguridad de información, aplicada al ciberespacio, sin embargo, se considera que hay aspectos que sobrepasan esta definición y se requiere incluir controles que permitan abordar la ciberseguridad de una manera más adecuada; el backup de un almacenamiento en nube —por ejemplo, ¿es seguridad de la información o ciberseguridad?

Y así, un gran sesgo conceptual nace y con ello las investigaciones y el esfuerzo de la ISO para abordar de la mejor manera las definiciones relacionadas al ciberespacio, es por esto que nace la ISO/IEC TR 27103:2018, para brindar orientación sobre cómo aprovechar los estándares existentes en la ciberseguridad;

pues en ella se define el ciberespacio como “esa parte de la seguridad de la información relacionada con TI” y por tanto, los estándares de seguridad y riesgos de la información son relevantes para la ciberseguridad, el documento brinda orientación sobre cómo aprovechar dichos estándares en un marco de ciberseguridad.

Otro aspecto importante de esta norma, y que es interpretable al cerrar estas brechas sobre seguridad de la información y ciberseguridad, es la responsabilidad de las empresas frente a los riesgos, y por ende, deben ser vistos como un tema organizacional principalmente; el documento describe la importancia de contar con un marco de ciberseguridad basado en riesgos, priorizado, flexible y centrado en resultados, a pesar de haber sido presentado como un informe técnico, la ISO/IEC TR 27103:2018 permitió la identificación de conceptos correlacionados con otros marcos populares, permitiendo deducir que las actividades previas de la organización en materia de ciberseguridad no son esfuerzos mal invertidos y que pueden ser reutilizadas en la definición de marcos de ciberseguridad basados en la ISO.

Posteriormente, en el 2020, nace la ISO/IEC 27100:2020 que plantea un nuevo enfoque a nivel de concepto y nuevas terminologías aplicables, y es aquí donde la ciberseguridad deja de ser un esfuerzo por la preservación de propiedades de seguridad de información (confidencialidad, integridad y disponibilidad) en el ciberespacio, y se define como salvaguardar a las personas, la sociedad, las organizaciones y las naciones de los ciber-riesgos, actualizando la concepción de seguridad orientada a proteger los activos de información, contra un concepto como el de “salvaguardar” que puede ser interpretado como mantener los riesgos en niveles adecuados. Y es así como el concepto de ciberseguridad a partir de la ISO/IEC 27100, cubre una mayor cantidad de ámbitos, incluyendo los relacionados con la vida de las personas y la infraestructura crítica.

En el 2021 se publica la ISO/IEC 27110:2021 que cubre la necesidad de identificar la responsabilidad de las organizaciones frente a riesgos de ciberseguridad, prestando especial interés en la importancia del contexto organizacional como columna vertebral para la ciberdefensa, y en este sentido, la ISO/IEC 27110:2021 detalla las especificaciones técnicas necesarias para diseñar un marco de ciberseguridad.

El estándar ofrece orientación para aquellos que dentro de las organizaciones crean marcos de ciberseguridad, definido como un conjunto de herramientas y actividades encaminadas a la seguridad en el ciberespacio, identificadas de manera organizada de acuerdo a las necesidades de las organizaciones, los requerimientos de las partes interesadas y el contexto en general.

El objetivo de la norma es garantizar que se utilice un conjunto mínimo de conceptos para definir marcos de ciberseguridad, alivianando carga a los creadores, aunando

que los conceptos de este estándar se encuentran perfectamente alineados con los de otros marcos existentes en el mundo, haciendo del marco resultante una herramienta interoperable con otras organizaciones, así como flexible y compatible con otras actividades y herramientas ya implementadas, garantizando la continuidad de los esfuerzos invertidos en dicho ámbito.

Otra característica relevante de la norma, es que aplica para creadores de marcos de ciberseguridad sin importar el tamaño, tipo o naturaleza de su organización, concepto que resalta de cierta medida, la importancia de conocer el contexto organizacional, ya que se viene hablando fuertemente del papel de la organización en la ciberdefensa desde la ISO/IEC 27103:2018.

Tomemos en consideración que todas las organizaciones sin importar su tamaño, tipo o naturaleza tiene una estructura organizacional con múltiples aspectos, por mencionar algunos: una alta gerencia como máximo ente organizacional, una gerencia corporativa, gerencia ejecutiva, que orientan operaciones, la administración entre otros, todo esto, para alcanzar los objetivos del negocio, sean financiero, de valor público, social, etc. esto hace que todas las organizaciones tengan, además, una inversión, infraestructura, partes interesadas, procesos y procedimientos que propende alcanzar dichos objetivos.

Un modelo genérico de organización que nos permita entender el contexto desde un aspecto estructurado es el siguiente:

Figura 1. Contexto organizacional

¿Cómo el entendimiento del contexto organizacional aporta a la ciberdefensa?; todos los esfuerzos en las organizaciones se centran en alcanzar sus objetivos; identificarlos permite reconocer las principales actividades y procesos para centrar los esfuerzos de ciberseguridad en aquellos que den frente a la misionalidad institucional, donde se aumenta el riesgo de ataques cibernéticos, todo esto sin dejar de lado otros aspectos de apoyo y administración.

El contenido de la norma ISO/IEC 27110:2021, da especial importancia al contexto organizacional, toda vez que se desea cubrir necesidades de protección a las personas, la comunidad y las empresas, más no alentar la creación de marcos de ciberseguridad enfocados únicamente a la información, identificando el entorno mixto del ejercicio misional entre lo convencional y lo virtual, pues sin importar su porcentaje, la presencia en el ciberespacio les aporta riesgos y amenazas a las organizaciones.

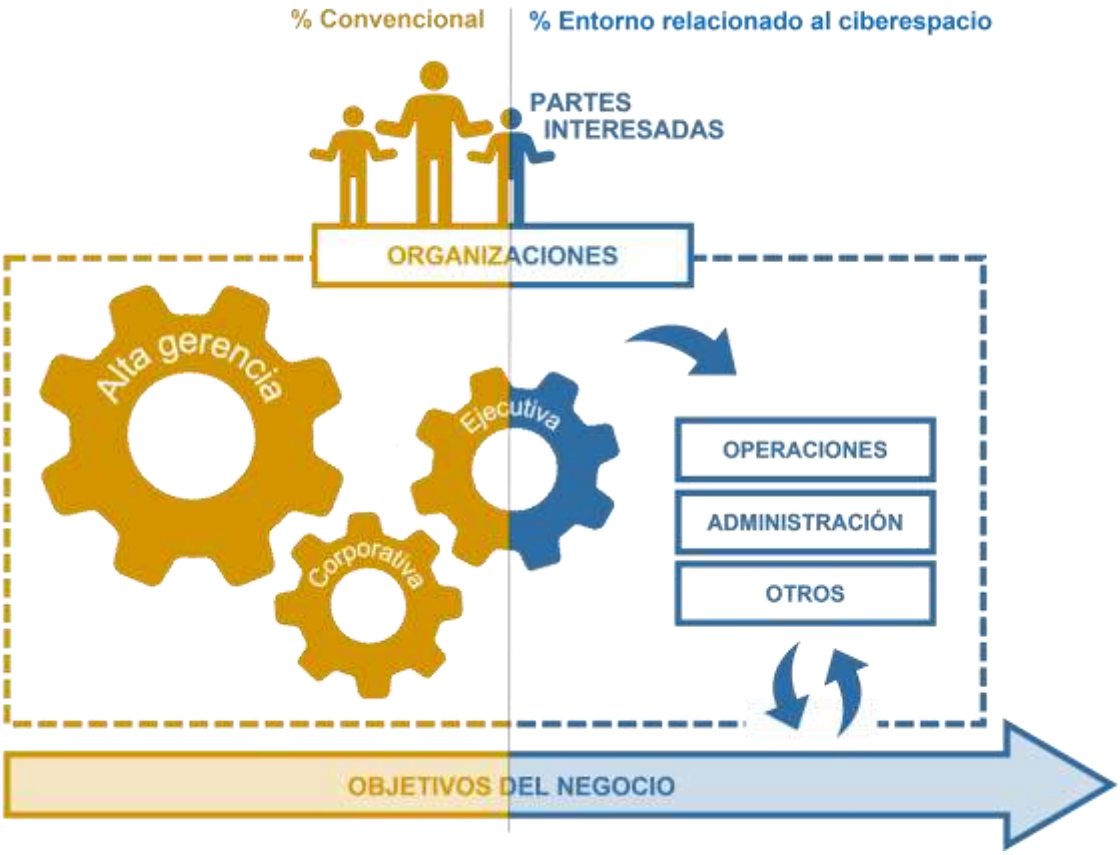


Figura 2. Presencia en el ciberespacio

Los correos electrónicos, las redes sociales y cualquier medio de conexión de red establecida dentro de la organización y no necesariamente relacionado a cumplir los objetivos del negocio, sino tal vez, actividades en red con intereses distintos;

comprender este porcentaje de participación en el ciberespacio es lo que nos permite abordar de manera apropiada la ciberseguridad, comprendiendo que al tener un espacio interconectado, existe la probabilidad que haya afectación de ciertos riesgos, y dependiendo del riesgo, así como del medio conectado a él, el efecto negativo o la principal consecuencia, puede ser a la persona, a la empresa, grupo de empresas, a la región o incluso al país, y en este sentido, se fortalece la necesidad crear marcos de ciberseguridad que aborde de manera adecuada los riesgos en las organizaciones y tomar acciones que permitan mantenerlos en los niveles aceptados.

Otra consideración importante en el entendimiento del contexto es que los riesgos nacen con las organizaciones, otros son nuevos como resultado de implementaciones tecnológicas y otros por actividades propias o indirectas, por ejemplo, el simple hecho de enviar un correo electrónico; más estos riesgos no emergen a partir del momento en que se toma conciencia o se evalúan, y probablemente han estado afectando de manera positiva o negativa desde el inicio de operaciones.

Dado lo anterior, se puede decir que el impacto negativo que tienen los ciberataques o las ciber amenazas, no están dirigidos a un área específica, sino, que impactan a los objetivos del negocio, adicionalmente, estas amenazas no necesariamente están enfocadas a ejecutar el ataque, factor que nos hace pensar que es necesario identificarlas desde su nivel de ataque, pues no es lo mismo si la penetración exitosa se hace en una infraestructura crítica a una que no lo sea.

Y entendiendo el contexto de la organización, muchos creadores de marcos de ciberseguridad han adaptado políticas, controles, herramientas y procedimientos para hacer frente a los ciberataques, estos modelos se hacen diversos dado que los marcos existentes en común, alientan la flexibilidad de su implementación, entre otras recomendaciones importantes como tomarse el tiempo de analizar y adaptar los controles que respondan de forma adecuada y coherente a las necesidades de la organización.

ISO/IEC 27110:2021 nace con el propósito de que las organizaciones empiecen a desplegar aspectos que mejoren su postura en ciberseguridad de manera organizada y coherente, para que los creadores de marcos alivien cargas en la definición de los mismos relacionadas a la definición de términos, permitiendo reunir aspectos comunes entre organizaciones y con ello generar interoperabilidad entre los marcos resultantes.

Estos aspectos en común, ya sean tamaño, limitantes, necesidades de cumplimiento, sistemas de información, protocolos, modelos de contratos etc. De acuerdo a la norma ISO/IEC 27110:2021, el creador debe tomarlos como requisitos, y entendidos de esta manera, determinarlo como un insumo del contexto para la creación del marco de ciberseguridad, sumando las necesidades y expectativas de

las partes interesadas, así como los lineamientos de la norma para estructurar un marco de ciberseguridad que reúna todos estos aspectos.

Los marcos de ciberseguridad resultantes deben estar desplegados bajo los conceptos: identificar, proteger, detectar, responder y recuperar, y estos a su vez no deben verse como etapas o fases, pues no son directrices obligatorias, por el contrario, la palabra “concepto” puede ser interpretada como algo que se debe entender, analizar y aplicar según sea el contexto.

Por otra parte, llama la atención que estos conceptos son igual a los de otro modelos de marcos existentes, entendiendo que la ISO/IEC 27110:2021 espera que dichos marcos resultantes no sean productos aislados, sino de fácil integración, ya sean con otros marcos basados en ISO/IEC 27110:2021 como los definidos bajo otros estándares populares, y así, un buen aporte de ISO/IEC 27110:2021 a los creadores de marcos de ciberseguridad con la definición de estos conceptos, es resaltar que las buenas prácticas se entienden, se conocen y se reutilizan.

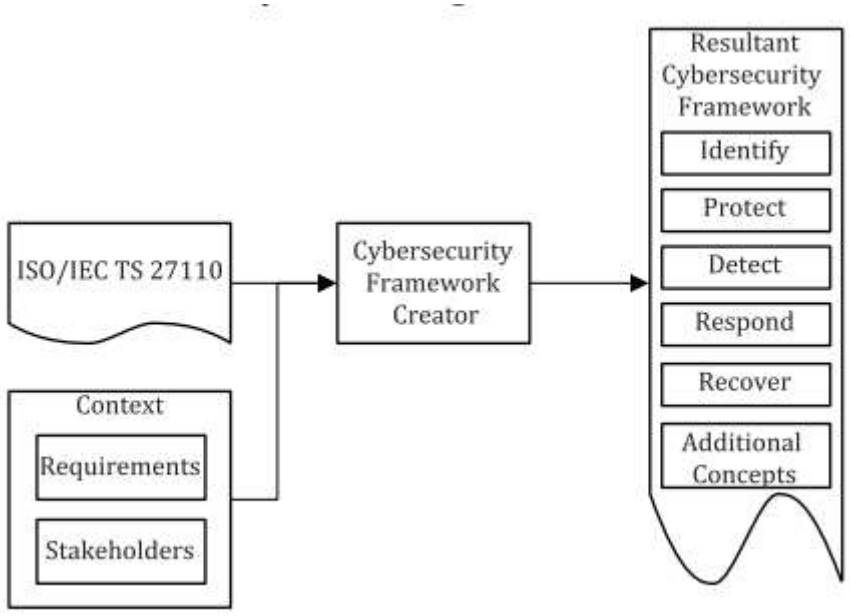


Figura 3. Estructura ISO/IEC 27110:2021

En síntesis, la ISO/IEC 27110:110, es una norma que permite identificar las ideas base para que los creadores de marcos de ciberseguridad tengan todos los insumos le que permitan definir marcos de ciberseguridad basado en los cinco conceptos, garantizando así, que el marco de ciberseguridad resultante sea comprensible, flexible, compatible e interoperable.

3.1.2 FASE 2: RECOLECCIÓN DE INFORMACIÓN

Una vez identificado el objetivo de la norma, se procedió a la recolección de referencias a controles y buenas prácticas existentes en estándares ISO y marcos populares, los cuales fueron organizados de acuerdo a los conceptos de la ISO/IEC 27110:2021 para la definición de marcos de ciberseguridad, que permitan reconocer las actividades a ejecutar en cada uno de ellos.

Categoría	Descripción	Referencia
Identificar	Inventario de información y otros activos asociados	ISO/IEC 27002:2022 5.9
		NIST SP 800-53 Rev 4 CM-8, PM-5
	Comunicación y flujo de datos mapeados	ISO/IEC 27002:2022 5.14
		NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
	Administración de los recursos (hardware, dispositivos, datos, tiempo, personal y software)	COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02
		ISO/IEC 27002:2022 5.12
		NIST SP 800-53 Rev 4 CP-2, RA-2, SA-14, SC-6
	Roles y responsabilidades de ciberseguridad de empleados y partes interesadas (empleados, proveedores, socios, clientes, etc...)	ISO/IEC 27002:2022 5.2
		NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Identificación de la cadena de suministro de la organización	ISO/IEC 27002:2022 5.19, 5.20, 5.21, 5.22
		NIST SP 800-53 Rev 4 CP-2, SA-12

	Identificación de la infraestructura crítica de la organización	ISO/IEC 27002:2022 Cláusula 4.1
		NIST SP 800-53 Rev 4 PM-8
	Establecer las prioridades para la misión, los objetivos y las actividades de la organización.	NIST SP 800-53 Rev 4 PM-11, SA-14
		COBIT 5 APO02.01, APO02.06, APO03.01
	Requerimientos de resiliencia para respaldar la prestación de servicios críticos (ataque, durante la recuperación, operaciones normales, etc..)	ISO/IEC 27002:2022 7.5, 5.29, 8.14
		NIST SP 800-53 Rev 4 CP-2, CP-11, SA-13, SA-14
	Inventario de plataformas y aplicaciones de software	ISO/IEC 27002:2022 5.9, 8.19
		NIST SP 800-53 Rev 4 CM-8, PM-5
	Lista de los sistemas de información externos	ISO/IEC 27002:2022 7.9
		NIST SP 800-53 Rev 4AC-20, SA-9
	Priorización de los recursos en función de la clasificación, criticidad y valor comercial.	ISO/IEC 27002:2022 5.12
		NIST SP 800-53 Rev 4 CP-2, RA-2, SA-14, SC-6
	Se establecen áreas y funciones para la prestación de servicios críticos	ISO/IEC 27002:2022 7.11, 7.12, 8.6
		NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

	La gobernanza y gestión del riesgo, abordan riesgos de ciberseguridad	ISO/IEC 27002:2022 Cláusula 6
		NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Identificar y documentar las vulnerabilidades de los activos	ISO/IEC 27002:2022 8.8, 5.36
		NIST SP 800-53 Rev 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	Identificar y documentar las amenazas internas y externas	ISO/IEC 27002:2022 Cláusula 6.1.2
		NIST SP 800-53 Rev 4 RA-3, SI-5, PM-12, PM-16
Proteger	Comunicación y capacitación a todos los usuarios de la organización	ISO/IEC 27002:2022 6.3, 8.7
		NIST SP 800-53 Rev 4 AT-2, PM-13
	Los usuarios con privilegios entienden sus roles y responsabilidades	ISO/IEC 27002:2022 5.2, 6,3
		NIST SP 800-53 Rev 4 AT-3, PM-13
	Los encargados de la seguridad física y cibernética entienden sus roles y responsabilidades	ISO/IEC 27002:2022 5.2, 6.3
		NIST SP 800-53 Rev 4 AT-3, IR-2, PM-13
	Manejo adecuado de la información para garantizar la disponibilidad	ISO/IEC 27002:2022 8.6, 8.14
		NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5

	Mecanismos para la verificación de la integridad del software, el firmware y la información.	ISO/IEC 27002:2022 8.7, 8.19, 8.26
		NIST SP 800-53 Rev 4 SC-16, SI-7
	El acceso físico a los activos de información está gestionados y protegidos	ISO/IEC 27002:2022 7.1, 7.2, 7.3, 7.5, 7.6, 7.8, 7.12, 7.9, 7.14,8.1
		NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
	Gestión de acceso remoto	ISO/IEC 27002:2022 8.1, 6.7, 7.9, 8.2, 5.14
		NIST SP 800-53 Rvdo. 4 AC-1, AC-17, AC-19, AC-20, SC-15
	Gestión de permisos y autorizaciones de acceso, incorporando los principios de mínimo privilegio y separación de funciones	ISO/IEC 27002:2022 6.8, 5.15, 8.2, 8.3, 8.18, 8.4
		NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
	Segregación y segmentación de la red	ISO/IEC 27002:2022 8.20, 8.22, 5.14, 8.26
		NIST SP 800-53 Rev 4 AC-4, AC-10, SC-7
	Autenticación de usuarios, dispositivos y otros activos	ISO/IEC 27002:2022 5.16, 5.17, 8.5, 5.17, 5.34
		NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA- 9, IA-10, IA-11
	Los altos ejecutivos entienden sus roles y responsabilidades	ISO/IEC 27002:2022 5.2, 6.3
		NIST SP 800-53 Rev 4 AT-3, PM-13

	Las copias de seguridad se encuentran protegidos	ISO/IEC 27002:2022 5.10
		NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
	Plan de protección contra fuga de datos	ISO/IEC 27002:2022 6.8, 5.29, 6.5, 5.13, 5.10, 5.15, 8.2, 8.3, 8.18, 8.4, 8.24, 7.5, 7.6, 7.8, 8.20, 8.22, 5.14, 6.6, 8.26
		NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
	Los entornos de desarrollo y pruebas están separados de producción	ISO/IEC 27002:2022 8.31
		NIST SP 800-53 Rev. 4 CM-2
Detectar	Análisis de los eventos para comprender los objetivos y métodos de ataque.	ISO/IEC 27002:2022 A.12.4.1, A.16.1.1, A.16.1.4
		NIST SP 800-53 Rev 4 AU-6, CA-7, IR-4, SI-4
	Determinar el impacto de los eventos	ISO/IEC 27002:2022 A.16.1.4
		NIST SP 800-53 Rev 4 CP-2, IR-4, RA-3, SI-4
	Monitoreo constante de la red para detectar posibles eventos de seguridad	COBIT 5 DSS01.03, DSS03.05, DSS05.07
		NIST SP 800-53 Rvdo. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
	Capacitar al personal para detectar posibles eventos de seguridad	ISO/IEC 27002:2022 A.12.4.1, A.12.4.3
		NIST SP 800-53 Rvdo. 4AC-2, AU-12, AU-13, CA-7, CM-10, CM-11

	Realizar escaneos de vulnerabilidades	ISO/IEC 27002:2022 A.12.6.1
		NIST SP 800-53 Rvdo. 4 RA-5
	Se establecen umbrales de alerta de incidentes	ISO/IEC 27002:2022 5.25
		NIST SP 800-53 Rvdo. 4 IR-4, IR-5, IR-8
	Monitoreo del entorno físico para detectar posibles eventos de seguridad	ISO/IEC 27002:2022 7.1, 7.2
		NIST SP 800-53 Rvdo. 4 CA-7, PE-3, PE-6, PE-20
	Detección de código malicioso	ISO/IEC 27002:2022 8.7
		NIST SP 800-53 Rev. 4 SI-3, SI-8
	Monitoreo de conexiones, dispositivos y software no autorizados utilizado por el personal	ISO/IEC 27002:2022 8.15, 8.30, 5.22
		NIST SP 800-53 Rvdo. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
	Se realizan pruebas de los procesos de detección	ISO/IEC 27002:2022 8.29
		NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
	Los procesos de detección se mejoran continuamente	ISO/IEC 27002:2022 5.27
		NIST SP 800-53 Rev. 4 , CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Responder	Ejecución del plan de respuesta durante o después de un incidente.	ISO/IEC 27002:2022 5.26
		NIST SP 800-53 Rvdo. 4 CP-2, CP-10, IR-4, IR-8
	Se debe informar los incidentes de acuerdo con los criterios establecidos.	ISO/IEC 27002:2022 5.5, 5,3
		NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
	Se debe clasificar el incidente de acuerdo con los planes de respuestas.	ISO/IEC 27002:2022 5.25
		NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
	Mitigación de los incidentes	ISO/IEC 27002:2022 8.7, 5.26
		NIST SP 800-53 Rev. 4IR-4
	Respuesta de los planes y lecciones aprendidas	ISO/IEC 27002:2022 5.27
		NIST SP 800-53 Rev 4CP-2, IR-4, IR-8
Recuperar	Ejecución del plan de respuesta durante o después de un incidente de seguridad.	ISO/IEC 27002:2022 5.26
		NIST SP 800-53 Rev 4 CP-10, IR-4, IR-8
	Plan de incorporación de lecciones aprendidas	ISO/IEC 27002:2022 5.27
		NIST SP 800-53 Rev 4CP-2, IR-4, IR-8

	Manejo de las relaciones publicas	COBIT 5 EDM03.02
		ISO/IEC 27002:2022 5.6
	Comunicación a las partes interesas internas y externas	ISO/IEC 27002:2022 Cláusula 7.4
		NIST SP 800-53 Rev. 4 CP-2, IR-4

Tabla 1. Mapeo general de controles

Adicionalmente, de acuerdo con la actualización de la norma ISO/IEC 27002 el 28 de febrero de 2022, y que afecta directamente los controles referenciados en la ISO/IEC 27110:2021, fue necesario realizar un mapeo de cada uno de los controles actualizados, creados y eliminados con el fin de poder brindar información reciente que responda de forma precisa y coherente a los conceptos del marco de ciberseguridad resultante.

ISO 27002:2013		**27002:2022**	
Cláusula	**Descripción**	**Cláusula**	**Descripción**
A.5	Políticas de seguridad de la información	5	Controles organizacionales
A.5.1.1	Políticas de seguridad de la información	5,1	Políticas de seguridad de la información
A.5.1.2	Revisión de las políticas de seguridad de la información		
A.6.1.1	Funciones y responsabilidades de la seguridad de la información	5,2	Funciones y responsabilidades de la seguridad de la información
A.6.1.2	Segregación de deberes	5,3	Segregación de deberes
A.6.1.3	Contacto con autoridades	5,5	Contacto con autoridades

A.6.1.4	Contacto con grupos de interés especial	5,6	Contacto con grupos de interés especial
Nuevo		5,7	la inteligencia
A.6.1.5 A.14.1.1	Seguridad de la información en la gestión de proyectos	5,8	Seguridad de la información en la gestión de proyectos
	Análisis y especificación de equipos de seguridad de la información		
A.6	Organización de la seguridad de la información	8	Controles tecnológicos
A.6.2.1 A.11.2.8	Dispositivos móviles (Movido a Gestión de activos)	8,1	Dispositivos de punto final de uso
	Equipo de uso desatendido		
A.6	Organización de la seguridad de la información	6	Controles de personas
A.6.2.2	Teletrabajo	6,7	Trabajo remoto
A.7	Seguridad de Recursos Humanos	6	Controles de personas
A.7.1.1	Proyección	6,1	Proyección
A.7.1.2	Equipos y condiciones de empleo	6,2	Equipos y condiciones de empleo
A.7.2.1	Responsabilidades de la gerencia	5,4	Responsabilidades de la gerencia
A.7.2.2	Información seguridad conciencia, educación y formación	6,3	Información seguridad conciencia, educación y formación

A.7.2.3	proceso disciplinario	6,4	proceso disciplinario
A.7.3.1	Terminación de responsabilidades por cambio de empleo	6,5	Responsabilidades después de la terminación del cambio de empleo
A.8	Gestión de activos	5	Controles organizacionales
A.8.1.1 A.8.1.2	Inventario de activos	5,9	Inventario de información y otros activos asociados
	Propiedad de los activos		
A.8.1.3 A.8.2.3	Uso aceptable de los activos	5,10	Uso aceptable de los activos y otros activos de información asociados
	manejo de activos		
A.8.1.4	Devolución de activos	5,11	Devolución de activos
A.8.2.1	Clasificación de la información	5,12	Clasificación de la información
A.8.2.2	Etiquetado de la información	5,13	Etiquetado de Información
A.8	Gestión de activos	7	Controles físicos
A.8.3.1	Gestión de soportes móviles	7,10	Medios de comunicación
A.8.3.2	Eliminación de medios	7,10	Medios de comunicación
A.8.3.3	Medios físicos transito	7,10	Medios de comunicación
A.9	Control de acceso	5	Controles organizacionales

A.9.1.1 A.9.1.2	Política de control de acceso	5,15	Control de acceso
	Acceso a redes y servicios de red		
A.9.2.1	Registro de usuario	5,16	Gestión de identidad
A.9.2.2 A.9.2.5 A.9.2.6	Acceso de uso	5,18	Derechos de acceso
	Revisión de los derechos de acceso		
	Eliminación o ajuste de las luces de acceso		
A.9	Control de acceso	8	Controles tecnológicos
A.9.2.3	Gestión de los derechos de acceso privilegiado	8,2	
A.9	Control de acceso	5	Controles organizacionales
A.9.2.4 A.9.3.1	Gestión de información de autenticación secreta de uso	5,17	Autenticación de información
	Uso de información de autenticación secreta		
A.9	Control de acceso	8	Controles tecnológicos
A.9.4.1	Información de acceso a la restricción	8,3	Información de acceso a la restricción

A.9.4.2	Pasos de inicio de sesión seguros	8,5	Autenticación segura
A.9	Control de acceso	5	Controles organizacionales
A.9.4.3	Sistema de gestión de contraseñas	5,17	Autenticación de información
A.9	Control de acceso	8	Controles tecnológicos
A.9.4.4	Uso de herramientas de administración del sistema	8,18	Uso de herramientas de administración del sistema
A.9.4.5	Control de acceso al código fuente de programas	8,4	Acceso al código fuente
A.10	criptografía	8	Controles tecnológicos
A.10.1.1 A.10.1.2	Política sobre el uso de controles criptográficos	8,24	Uso de la criptografía
	Gestión de claves		
A.11	Seguridad física y ambiental	7	Controles físicos
A.11.1.1	Perímetro de seguridad física	7,1	Perímetro de seguridad física
A.11.1.2 A.11.1.6	Controles de entidades físicas	7,2	Controles de entidades físicas
	Áreas de entrega y carga		
A.11.1.3	Seguridad de oficinas, salas e instalaciones	7,3	Seguridad de oficinas, salas e instalaciones
Nuevo		7,4	Vigilancia de la seguridad física

A.11.1.4	Protección contra amenazas externas y ambientales	7,5	Protección contra amenazas físicas y ambientales
A.11.1.5	Trabajando en áreas seguras	7,6	Trabajando en áreas seguras
A.11.2.1	Emplazamiento y protección de equipos	7,8	Emplazamiento y protección de equipos
A.11.2.2	Utilidades de apoyo	7,11	Utilidades de apoyo
A.11.2.3	Seguridad del cableado	7,12	Seguridad del cableado
A.11.2.4	Mantenimiento de equipo	7,13	Mantenimiento de equipo
A.11.2.5	Eliminación de activos	**Eliminado**	**Eliminado**
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	7,9	Seguridad de activos fuera de las instalaciones
A.11.2.7	Eliminación segura del uso de equipo	7,14	Eliminación segura del uso de equipo
A.11.2.8	Equipo de uso desatendido	8,1	Dispositivos de punto final de uso
A.11.2.9	Política de escritorio limpio y pantalla limpia	7,7	Escritorio limpio, política de pantalla limpia
A.12	Seguridad de las operaciones	5	Controles organizacionales
A.12.1.1	Procedimientos operativos documentados	5,37	Procedimientos operativos documentados
A.12	Seguridad de las operaciones	8	Controles tecnológicos
A.12.1.2	Gestión del cambio	8,32	Gestión del cambio
A.12.1.3	Gestión de capacidad	8,6	Gestión de capacidad
A.12.1.4	Separación de entornos de desarrollo, pruebas y	8,31	Separación de entornos de desarrollo, prueba y

	operativos		producción
A.12.2.1	Controles contra malware	8,7	Protección contra malware
A.12.3.1	Copia de seguridad de la información	8,13	Copia de seguridad de la información
A.12.4.1 A.12.4.2 A.12.4.3	El registro de eventos	8,15	Inicio sesión
	Protección de la información de registro		
	Registros de administración y operación del sistema		
Nuevo		8,16	Actividades de seguimiento
A.12.4.4	Sincronización de reloj	8,17	Sincronización de reloj
A.12.5.1	Instalación de software en sistemas operativos	8,19	Instalación de software en sistemas operativos
A.12.6.1	Gestión de vulnerabilidades técnicas	8,8	Gestión de vulnerabilidades técnicas
Nuevo		8,9	Gestión de configuración
Nuevo		8,10	Eliminación de información
Nuevo		8,11	Enmascaramiento de datos
Nuevo		8,12	Prevención de fuga de datos
A.13	Seguridad de las comunicaciones	8	Controles tecnológicos

A.13.1.1	Controles de red	8,20	Controles de red
A.13.1.2	Seguridad de los servicios de red	8,21	Seguridad de los servicios de red
A.13.1.3	Segregación en redes	8,22	Segregación en redes
Nuevo		8,23	Filtrado web
A.13	Seguridad de las comunicaciones	5	Controles organizacionales
A.13.2.1 A.13.2.2 A.13.2.3	Políticas y procedimientos de información	5,14	Intercambio de información
	Acuerdos sobre información intercambios		
	Mensajería electrónica		
A.13	Seguridad de las comunicaciones	6	Controles de personas
A.13.2.4	Confidencialidad de los acuerdos de no divulgación	6,6	Confidencialidad de los acuerdos de no divulgación
A.14	Adquisición, desarrollo y mantenimiento de sistemas y software	8	Controles tecnológicos
A.14.1.1	Equipos de seguridad de la información, análisis y especificaciones	5,8	Seguridad de la información en la gestión de proyectos
A.14.1.2 A.14.1.3	Seguridad de servicios de aplicaciones en redes públicas	8,26	Equipos de seguridad de la aplicación

	Protección de las transacciones por redes		
A.14.2.1	Política de desarrollo seguro de software	8,25	Ciclo de vida de desarrollo seguro
A.14.2.2	Procedimientos de control de cambio del sistema	8,32	Gestión del cambio
A.14.2.5	Principios de ingeniería de sistemas de seguridad	8,27	Principios de ingeniería y arquitectura del sistema de seguridad
Nuevo		8,28	Codificación segura
A.14.2.6	Entorno de desarrollo seguro	8,31	Separación de entornos de desarrollo, prueba y producción
A.14.2.7	Desarrollo subcontratado	8,30	Desarrollo subcontratado
A.14.2.8 A.14.2.9	Pruebas de seguridad del sistema	8,29	Pruebas de seguridad en desarrollo y aceptación.
	Pruebas de aceptación del sistema		
A.14.3.1	Protección de datos de prueba	8,33	Información de prueba
A.15	Relaciones de suministro	5	Controles organizacionales
A.15.1.1	Seguridad de la información en las relaciones de suministro	5,19	Seguridad de la información en las relaciones de suministro
A.15.1.2	Agregar seguridad dentro de los acuerdos de suministro	5,20	Agregar seguridad dentro de los acuerdos de suministro
A.15.1.3	Cadena de suministro de tecnologías de la información y las comunicaciones	5,21	Gestión de la seguridad de la información en la cadena de suministro de las TIC

A.15.2.1 A.15.2.2	Seguimiento y revisión de los servicios de abastecimiento	5,22	Supervisión, revisión y gestión de cambios de los servicios de suministro
	Gestión de cambios en el suministro		
	servicios		
Nuevo		5,23	Seguridad de la información para el uso de servicios en la nube
A.16	Administración de incidentes	5	Controles organizacionales
A.16.1.1	Responsabilidades y procedimientos	5,24	Planificación y gestión de incidentes de seguridad de la información
A.16	Administración de incidentes	6	Controles de personas
A.16.1.2 A.16.1.3	Notificación de eventos de seguridad de información	6,8	Señalización de eventos de seguridad de información
	Informar sobre las debilidades de seguridad de la información		
A.16	Administración de incidentes	5	Controles organizacionales
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	5,25	Evaluación y decisión sobre eventos de seguridad de la información
A.16.1.5	Respuesta a incidentes de seguridad de la información	5,26	Respuesta a incidentes de seguridad de la información
A.16.1.6	Aprender de la información incidentes de seguridad	5,27	Aprender de la información incidentes de seguridad

A.16.1.7	Recolección de evidencia	5,28	Recolección de evidencia
A.17	Aspectos de seguridad de la información de la continuidad del negocio	5	Controles organizacionales
A.17.1.1 A.17.1.2 A.17.1.3	Planificación de la continuidad de la seguridad de la información	5,29	Seguridad de la información durante la interrupción
	Implementación de la continuidad de la seguridad de la información		
	Verificar, revisar y evaluar la continuidad de la seguridad de la información		
Nuevo		5,30	Preparación TIC para la continuidad del negocio
A.17	Aspectos de seguridad de la información de la continuidad del negocio	8	Controles tecnológicos
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	8,14	Redundancia de instalaciones de procesamiento de información
A.18	Cumplimiento	5	Controles organizacionales
A.18.1.1 A.18.1.5	Identificación de los elementos legislativos y contractuales aplicables	5,31	Identificación de los elementos legislativos y contractuales aplicables
	Regulación de los controles criptográficos		
A.18.1.2	Derechos de propiedad intelectual	5,32	Derechos de propiedad intelectual

A.18.1.3	Protección de registros	5,33	Protección de registros
A.18.1.4	Privacidad y protección de información personal identificable	5,34	Privacidad y protección de PII
A.18.2.1	Revisión independiente de la seguridad de la información	5,35	Revisión independiente de la seguridad de la información
A.18.2.2	Cumplimiento de políticas y estándares de seguridad	5,36	Cumplimiento de políticas y estándares de seguridad
A.18.2.3	Revisión del cumplimiento técnico	5.36. 8.8	Revisión del cumplimiento técnico

Tabla 2. Mapeo ISO/IEC 27002:2022

3.1.3 FASE 3: ELABORACIÓN DEL PRODUCTO

La ISO/IEC TS 27110/2021 tiene como objetivo garantizar el uso mínimo de conceptos en la creación de marcos de ciberseguridad, aliviando cargas de trabajo a los creadores, permitiendo entre otros beneficios, la interoperabilidad con otros marcos e implementaciones ya realizadas en la organización.

La **GUIA PARA EL ABORDAJE ISO/IEC TS 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD** brinda una interpretación sencilla de la norma ISO/IEC TS 27110/2021, con la intención de ser comprensible por todas las partes interesadas, incluso, si el creador del marco de ciberseguridad no es especialista en seguridad de la información, pues su alcance no es limitado al tamaño, tipo o naturaleza de las empresas.

En la primera sección de la guía se explica los conceptos básicos para tener en cuenta en la definición de marcos de ciberseguridad basados en la ISO/IEC 27110:2021.

Un **Marco de Ciberseguridad** es el conjunto de documentos y herramientas empleadas para hacer frente a los ciberataques con el reto de proteger a los usuarios y las organizaciones. Y en ese sentido, quienes producen marcos de ciberseguridad se les denomina “creadores de marcos de ciberseguridad”.

La ISO (Organización Internacional de Normalización) y la CIE (Comisión Electrónica Internacional) publicaron en febrero de 2021 la **ISO/IEC TS 27110:2021** con el objetivo de garantizar que se utilicen un conjunto mínimo de conceptos en la definición de marcos de ciberseguridad permitiendo la armonización e interoperabilidad entre ellos.

El documento **ISO/IEC TS 27110:2021** especifica las directrices para desarrollar un marco de ciberseguridad. Es aplicable a los creadores de marcos de ciberseguridad independientemente del tipo, tamaño o naturaleza de sus organizaciones.

Las características del marco resultante deben ser:

Flexible: Para permitir que existan múltiples tipos de marcos de ciberseguridad y partiendo de lo que ya está implementado en las organizaciones.

Compatible: Que permita alinearse de forma correcta y pertinente con otros marcos de ciberseguridad

Interoperable: Para permitir que sean válidos múltiples usos de un marco de ciberseguridad

En la siguiente sección, se da una interpretación a los conceptos de la norma, detallando el alcance aspectos relevantes a tener en cuenta y algunos ejemplos que permitan identificar las categorías y subcategorías según sea el resultado del análisis del contexto.

Identificar

El concepto de identificar comprende todas las actividades que permiten la comprensión del contexto empresarial, los intereses, y en sí, conocer el ecosistema de la ciberseguridad actual de las organizaciones con el objetivo de analizar, identificar y evaluar los riesgos, amenazas y vulnerabilidades; el creador de marcos de ciberseguridad debe tener en cuenta la evolución de las ciber amenazas y las tecnologías emergentes, identificando la mayor cantidad de escenarios predictivos posibles según sea el análisis, esto permite mayor rango de obsolescencia del marco y aplicabilidad múltiple.

Tenga en cuenta que identificar es el inicio de todo, una evaluación eficaz de los riesgos permite mitigar los sesgos resultantes en los marcos de ciberseguridad a causa de una mala planeación, tómese el tiempo para resaltar la mayor cantidad de factores, principalmente los relacionados con la presencia de la organización, sus personas, la información, sus funciones y recursos en el ciberespacio, permítase crear todos los escenarios que vea conveniente y súmelos al marco, algunos ejemplos pueden ser:

- Análisis, identificación y evaluación de riesgos
- Gobernanza
- Activos de información

Proteger

En este concepto se pretende no solo salvaguardar a las empresas, sino a las personas que hacen parte de ella y que tienen presencia en el ciberespacio, también se busca asegurar que los controles preventivos están funcionando, puede contener muchas categorías y actividades relacionadas con la protección de los recursos, contra el uso inadecuado intencional o no.

De la misma manera, se pueden incluir controles para la seguridad de los sistemas tradicionales, el creador de marcos de ciberseguridad debe determinar el alcance para proteger, teniendo en cuenta todos los escenarios identificados, con la libertad de crear cuantas categorías sean convenientes considerando la protección de las personas, los procesos y la tecnología, algunos ejemplos de categorías pueden ser:

- Capacitación y sensibilización
- Gestión de acceso
- Gestión de los riesgos

Detectar

Los marcos de ciberseguridad resultantes deben proveer a la organización los recursos necesarios para desarrollar la capacidad de observar proactivamente los cambios en los comportamientos, estado, tráfico y procesamiento de sus recursos; sin importar si son cambios internos o externos, intencionales o no, comprender estas variaciones del panorama permite a las organizaciones realizar las respectivas actualizaciones en las políticas, dando valor al marco implementado, de igual manera, el concepto de detección puede incluir la supervisión de recursos tradicionales y la detección de ciberataques.

Algunas categorías para considerar incluyen:

- Monitoreo
- Procesos de detención
- Vigilancia de seguridad

No importa si los esfuerzos previos de la organización para la ciberseguridad están centrados en los sistemas o en los procesos, el creador de marco de ciberseguridad sebe determinar la conducta apropiada basado en el principio de flexibilidad de la ISO/IEC TS 27110/2021

Responder

En este concepto se deben incluir todas las categorías que se consideren pertinentes asociadas a las actividades que permitan dar respuesta a los eventos de ciberseguridad; categorizarlas permite a las organizaciones evaluar y remediar los eventos de ciberseguridad en función de sus necesidades, recursos, partes

interesadas y requisitos específicos.

El creador del marco de ciberseguridad puede considerar conceptos tradicionales de respuesta a incidentes, políticas, procedimientos y planes, algunas categorías pueden ser:

- Análisis de incidentes
- Comunicaciones
- Mejora continua
- Procedimientos de mitigación
- Plan de respuesta

Recuperar

Recuperar hace referencia al desarrollo de actividades que permitan restaurar el negocio, las comunicaciones, los servicios, reparar los sistemas, restablecer la reputación; se debe tener en cuenta que recuperar no solo se trata de reactivo, por el contrario, la planeación y ejecución eficaz y eficiente de las actividades de recuperación permiten que este concepto se vuelva proactivo.

“Es posible que los servicios se hayan degradado a raíz de un incidente de ciberseguridad. "El concepto de recuperación es una oportunidad para proporcionar orientación sobre cómo restaurar esos servicios. Los servicios pueden ser de naturaleza técnica o de gestión. Los activos pueden haber alcanzado un estado de funcionamiento inoperable o no deseado.

Por lo anterior, algunos ejemplos de categorías podrían incluir:

- Plan de recuperación
- Comunicaciones

Mediante una explicación simple, se detalla cómo crear una estructura de marco de ciberseguridad basada en referencias a normas ISO y otra en una combinación coherente de otros estándares y marcos existente.

Hágalo fácil, organice todas las actividades de ciberseguridad y seguridad de la información que se hayan implementado y las que de acuerdo al análisis del contexto se considere importante implementar, diseñe una estructura utilizando los conceptos previamente descritos e incluya nuevos conceptos si así lo considera, divida por categorías y subcategorías y permita que sea comprensible a todas las partes interesadas; no importa el tamaño del marco de ciberseguridad resultante, todo depende del nivel de detalle al que se quiera llegar.

Por último, referencie en su estructura para cada categoría, los controles, documentos o herramientas que respondan de manera coherente a las categorías definidas.

Tenga en cuenta que existen diversos marcos de ciberseguridad en el mercado que son interoperables con los modelos basados en ISO 27110:2021 y de los cuales se pueden adoptar controles y buenas prácticas, por otra parte, tenga en cuenta que los controles de ciberseguridad basados en ISO deben ser consultados en la ISO/IEC 27002:2022 y complementados por las buenas prácticas de la ISO/IEC 27005:2018 y la ISO/IEC 31000:2018 para el análisis, identificación y evaluación del riesgo.

Así las cosas, dos formas de diseñar marcos de ciberseguridad basados en ISO/IEC 27110:2021 son:

1. Referenciación de otras normas ISO/IEC, identificando los conceptos base, dividiendo por categorías y referenciando de la manera más detallada posible la/las cláusulas que identifiquen de forma adecuada, precisa y pertinente la directriz, el control o la especificación técnica, algunas variables a incorporar incluyen:

    - Concepto
    - Categoría
    - Descripción
    - Subcategoría
    - Referencia ISO/IEC

2. Dado que el marco resultante debe poseer el principio de flexibilidad, compatibilidad e interoperabilidad, puede incluir un diseño genérico que referencie otras normas o procedimientos ya implementados, para no empezar de “cero”, organiza por categorías y detalle las características que son importantes a tener en cuenta; no olvide proporcionar un marco de ciberseguridad comprensible a todas las partes interesadas.

    Las variables pueden ser:

    - Concepto
    - Categoría
    - Descripción
    - Actividades

Por último, la **GUIA PARA EL ABORDAJE ISO/IEC TS 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD** mediante un ejemplo de marco de ciberseguridad básico, resalta las categorías y referencias ISO aplicables a cada uno de los conceptos de la norma, permitiendo a los creadores de marcos y a las partes interesadas tener claridad sobre algunos controles y buenas prácticas aplicables según corresponda.

IDENTIFICAR		
Categoría: Gestión del riesgo		
SUBCATEGORIA	DESCRIPCCION	REFERENCIA
Activos de Información	Inventario de información y otros activos asociados	ISO/IEC 27002:2022 CLAUSULA 5.9
	Comunicación y flujo de datos mapeados	ISO/IEC 27002:2022 CLAUSULA 5.14
	Administración de los recursos (hardware, dispositivos, datos, tiempo, personal y software)	ISO/IEC 27002:2022 CLAUSULA 5.12
	Roles y responsabilidades de ciberseguridad de empleados y partes interesadas (empleados, proveedores, socios, clientes, etc...)	ISO/IEC 27002:2022 CLAUSULA 5.2
	Inventario de plataformas y aplicaciones de software	ISO/IEC 27002:2022 CLAUSULA 5.9, 8.19
	Lista de los sistemas de información externos	ISO/IEC 27002:2022 CLAUSULA 7.9
Análisis, identificación y evaluación del riesgo	Identificación de la cadena de suministro de la organización	ISO/IEC 27002:2022 CLAUSULA 5.19, 5.20, 5.21, 5.22
	Identificación de la infraestructura critica de la organización	ISO/IEC 27002:2022 CLAUSULA Cláusula 4.1

	Requerimientos de resiliencia para respaldar la prestación de servicios críticos (ataque, durante la recuperación, operaciones normales, etc...)	ISO/IEC 27002:2022 CLAUSULA 7.5, 5.29, 8.14
	Priorización de los recursos en función de la clasificación, criticidad y valor comercial.	ISO/IEC 27002:2022 CLAUSULA 5.12
	Evaluación del riesgo de vulnerabilidades y amenazas internas y externas.	ISO/IEC 27002:2022 Cláusula 6.1.2, 8.8, 5.36 ISO/IEC 27005:2018 ISO/IEC 31000:2018
Gobernanza	Se establecen áreas y funciones para la prestación de servicios críticos	ISO/IEC 27002:2022 CLAUSULA 7.11, 7.12, 8.6
	La gobernanza y gestión del riesgo, abordan riesgos de ciberseguridad	ISO/IEC 27002:2022 CLAUSULA Cláusula 6
	Identificar y documentar las vulnerabilidades de los activos	ISO/IEC 27002:2022 CLAUSULA 8.8, 5.36
	Identificar y documentar las amenazas internas y externas	ISO/IEC 27002:2022 CLAUSULA Cláusula 6.1.2
PROTEGER		
Categoría: Usuarios y permiso		
SUBCATEGORIA	DESCRIPCCION	REFERENCIA
Capacitación y sensibilización	Comunicación y capacitación a todos los usuarios de la organización	ISO/IEC 27002:2022 CLAUSULA 6.3, 8.7

	Los encargados de la seguridad física y cibernética entiende sus roles y responsabilidades	ISO/IEC 27002:2022 CLAUSULA 5.2, 6.3
	Los altos ejecutivos entienden sus roles y responsabilidades	ISO/IEC 27002:2022 CLAUSULA 5.2, 6.3
	Plan de protección contra fuga de datos	ISO/IEC 27002:2022 CLAUSULA 6.8, 5.29, 6.5, 5.13, 5.10, 5.15, 8.2, 8.3, 8.18, 8.4, 8.24, 7.5, 7.6, 7.8, 8.20, 8.22, 5.14, 6.6, 8.26
	Los usuarios con privilegios entienden sus roles y responsabilidades	ISO/IEC 27002:2022 CLAUSULA 5.2, 6,3
Gestión de acceso	El acceso físico a los activos de información están gestionados y protegidos	ISO/IEC 27002:2022 CLAUSULA 7.1, 7.2, 7.3, 7.5, 7.6, 7.8, 7.12, 7.9, 7.14,8.1
	Gestión de acceso remoto	ISO/IEC 27002:2022 CLAUSULA 8.1, 6.7, 7.9, 8.2, 5.14
	Gestión de permisos y autorizaciones de acceso, incorporando los principios de mínimo privilegio y separación de funciones	ISO/IEC 27002:2022 CLAUSULA 6.8, 5.15, 8.2, 8.3, 8.18, 8.4
	Autenticación de usuarios, dispositivos y otros activos	ISO/IEC 27002:2022 CLAUSULA 5.16, 5.17, 8.5, 5.17, 5.34

Gestión del riesgo	Manejo adecuado de la información para garantizar la disponibilidad	ISO/IEC 27002:2022 CLAUSULA 8.6, 8.14
	Mecanismos para la verificación de la integridad del software, el firmware y la información.	ISO/IEC 27002:2022 CLAUSULA 8.7, 8.19, 8.26
	Segregación y segmentación de la red	ISO/IEC 27002:2022 CLAUSULA 8.20, 8.22, 5.14, 8.26
	Las copias de seguridad se encuentran protegidos	ISO/IEC 27002:2022 CLAUSULA 5.10
	Los entornos de desarrollo y pruebas están separados de producción	ISO/IEC 27002:2022 CLAUSULA 8.31
DETECTAR		
Categoría: Vigilancia de seguridad - anomalías		
SUBCATEGORIA	DESCRIPCCION	REFERENCIA
Monitoreo	Capacitar al personal para detectar posibles eventos de seguridad	ISO/IEC 27002:2022 CLAUSULA A.12.4.1, A.12.4.3
Proceso de detención	Análisis de los eventos para comprender los objetivos y métodos de ataque.	ISO/IEC 27002:2022 CLAUSULA A.12.4.1, A.16.1.1, A.16.1.4

	Realizar escaneos de vulnerabilidades	ISO/IEC 27002:2022 CLAUSULA A.12.6.1
	Se establecen umbrales de alerta de incidentes	ISO/IEC 27002:2022 CLAUSULA 5.25
	Monitoreo del entorno físico para detectar posibles eventos de seguridad	ISO/IEC 27002:2022 CLAUSULA 7.1, 7.2
	Detección de código malicioso	ISO/IEC 27002:2022 CLAUSULA 8.7
	Se realizan pruebas de los procesos de detección	ISO/IEC 27002:2022 CLAUSULA 8.29
Vigilancia de seguridad	Determinar el impacto de los eventos	ISO/IEC 27002:2022 CLAUSULA A.16.1.4
	Monitoreo de conexiones, dispositivos y software no autorizados utilizado por el personal	ISO/IEC 27002:2022 CLAUSULA 8.15, 8.30, 5.22
	Los procesos de detección se mejoran continuamente	ISO/IEC 27002:2022 CLAUSULA 5.27

RESPONDER		
Categoría: Atención de incidente		
SUBCATEGORIA	DESCRIPCCION	REFERENCIA
Análisis de incidentes	Se debe clasificar el incidente de acuerdo con los planes de respuestas.	ISO/IEC 27002:2022 CLAUSULA 5.25
Comunicaciones	Se debe informar los incidentes de acuerdo con los criterios establecidos.	ISO/IEC 27002:2022 CLAUSULA 5.5, 5,3
Mejora continua	Respuesta de los planes y lecciones aprendidas	ISO/IEC 27002:2022 CLAUSULA 5.27
Procedimientos de Mitigación	Mitigación de los incidentes	ISO/IEC 27002:2022 CLAUSULA 8.7, 5.26
Plan de respuesta	Ejecución del plan de respuesta durante o después de un incidente.	ISO/IEC 27002:2022 CLAUSULA 5.26
RECUPERAR		
Categoría: Recuperación de eventos		
SUBCATEGORIA	DESCRIPCCION	REFERENCIA
Plan de recuperación	Ejecución del plan de respuesta durante o después de un incidente de seguridad.	ISO/IEC 27002:2022 CLAUSULA 5.26

	Plan de incorporación de lecciones aprendidas	ISO/IEC 27002:2022 CLAUSULA 5.27
Comunicaciones	Manejo de las relaciones publicas	ISO/IEC 27002:2022 CLAUSULA 5.6
	Comunicación a las partes interesas internas y externas	ISO/IEC 27002:2022 CLAUSULA Cláusula 7.4

Tabla 3. Ejemplo de marco

3.2 ALCANCES Y LIMITACIONES

El alcance del proyecto es facilitar a los creadores de marcos y a las empresas una guía para abordar de forma adecuada la norma ISO/IEC 27110:2021 para la creación de marcos de ciberseguridad, el documento permitirá interpretar la norma de forma clara y concisa reuniendo los conceptos que se deben aplicar para satisfacer los principios de flexibilidad, compatibilidad e interoperabilidad aplicables en la materia y que permitirán desarrollar un marco basado en las mejores prácticas.

La implementación de esta norma ISO en las organizaciones es voluntaria y opcional, por tanto, esta guía solo constituye una interpretación de la norma, brindando una propuesta de marco de ciberseguridad básico, el cual debe ser complementado de acuerdo al análisis del contexto.

4 PRODUCTOS A ENTREGAR

Como resultado de la investigación, se generaron dos (2) productos: por un lado la Guía para el abordaje ISO/IEC TS 27110:2021 creación de marcos de ciberseguridad, la cual orienta a los creadores de marcos de ciberseguridad en los conceptos necesarios para la definición de modelos basados en en las buenas prácticas de la Organización Internacional de Estandarización (ISO), por otra parte, se hace entrega del articulo IEEE que reúne los puntos importantes de la investigación.

5 ENTREGA DE RESULTADOS E IMPACTOS

Como resultado del análisis, se hizo un mapeo general de las buenas prácticas ISO y las encontradas en otros marcos, con el propósito de identificar qué otros controles distintos a ISO responden de forma coherente e interoperable con los marcos resultantes basados en ISO/IEC 27110:2021 y una vez identificados, se diseña una guía con controles actualizados basados en 27002:2022, con una estructura sencilla de marco de ciberseguridad, la cual, a manera de ejemplo, busca orientar a los creadores en la definición de sus propios marcos, teniendo en cuenta que el marco final, debe estar coordinado y alineado con el análisis realizado al contexto organizacional.

La **GUIA PARA EL ABORDAJE ISO/IEC TS 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD** brinda una interpretación sencilla de la norma ISO/IEC TS 27110/2021, con la intención de ser comprensible por todas las partes interesadas, pues su alcance no es limitado al tamaño, tipo o naturaleza de las empresas; conozca cómo abordar la norma, una interpretación clara sobre cada uno de los conceptos sugeridos y descubra qué variables podría emplear de acuerdo al contexto de su empresa.

Por último, al final del documento encontrará un práctico ejemplo de categorías y subcategorías para la creación de un marco de ciberseguridad basado en la ISO/TS 27110:2021, tanto su descripción como las referencias ISO que le ayudarán a organizar las actividades de ciberseguridad en su organización.

La guía puede ser consultada y descargada a través del siguiente QR:

Figura 4. QR guía

6 NUEVAS ÁREAS DE ESTUDIOS

Es importante que las empresas mejoren su postura en ciberseguridad, es por esto que la GUIA PARA EL ABORDAJE ISO/IEC TS 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD reúne todos los conceptos basados en ISO/TS 27110:2021 para orientar a los creadores de marcos en la definición de modelos ordenados y estructurados.

la GUIA PARA EL ABORDAJE ISO/IEC TS 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD, puede emplearse para que los creadores de marcos de ciberseguridad estructuren modelos aplicables a empresas o grupos de empresas basados en 27110 y a partir de los ejemplos descritos, el cual sirve como base para estructuras complejas, detalladas y que responda de forma adecuada a los requisitos y necesidades del contexto organizacional y las parte interesadas

7 CONCLUSIONES

La ISO/IEC TS 27110:2021 se alinea de manera coherente con otros marcos de ciberseguridad existentes, las empresas que ya tienen implementado de forma parcial o total otros marcos, pueden complementarlo de manera interoperable y compatible, sin riesgo de perder los esfuerzos de la organización previamente invertidos.

La **GUIA PARA EL ABORDAJE ISO/IEC TS 27110:2021 CREACIÓN DE MARCOS DE CIBERSEGURIDAD** permite abordar los conceptos necesarios para la definición de marcos de ciberseguridad basado en normas ISO, así mismo, proporciona un lenguaje sencillo y referencias a controles que apoyen su construcción.

8 BIBLIOGRAFÍA

1. *Organización Internacional de Normalización* . (2021). Iso.Org. https://www.iso.org/home.html
2. Guerrero-Rincón, BL (2018). *Análisis de la relación costo - beneficio en el diseño e Implementación del sistema de gestión de calidad ISO 27001 en la empresa Gfi informática Colombia SAS* . Facultad de Ciencias Económicas y Administrativas.
3. Guzmán-Solano, SL (2019). Guía para la implementación de la norma ISO 27032 . Facultad de Ingeniería.
4. IsecT Ltd. www. isect.com. (Dakota del Norte). Marcos de seguridad cibernética ISO / IEC 27110 . Iso27001security.Com. Obtenido el 21 de noviembre de 2021 de https://www.iso27001security.com/html/27110.html
5. (Dakota del Norte). Iteh.Ai. Obtenido el 21 de noviembre de 2021 de https://cdn.standards.iteh.ai/samples/72435/2af38718e8ec47efa09287796b9da63c/ISO-IEC-TS-27110-2021.pdf
6. PROYECTO DE TRABAJO DE GRADO . Edu.co. Recuperado el 14 de diciembre de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/25743/1/TG-20203-13%20-%20DIANA%20SALAMANCA-JAIME%20ROZO%20TRABAJO%20DE% 20GRADO.pdf
7. Edu.co. Recuperado el 14 de diciembre de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/23326/1/Proyecto%20-%20AUDITORIA%20A%20LA%20SI%20DE%20ANS%20COMUNICACIONES%20ENTREGA% 20FINAL.pdf
8. Edu.co. Recuperado el 14 de diciembre de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/15240/1/Esp%20Auditoria%20de%20sistemas.pdf
9. Edu.co. Recuperado el 14 de diciembre de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/23388/1/RECOMENDACIONES%20DE%20SEGURIDAD%20PARA%20LOS%20SERVICIOS%20DE%20COMPUTACION%20EN%20LA%20NUBE .pdf
10. *VIGILANDO LA SEGURIDAD DE LA INFORMACIÓN* . Copant.org. Recuperado el 14 de diciembre de 2021, de https://copant.org/phocadownload/iso_lt_2020/2020-12-16%20-%20VIGILANDO%20LA%20SEGURIDAD%20DE%20LA%20INFORMACIN .pdf
11. *Martínez, V. (2019, 11 de abril). 5 marcos de ciberseguridad que los auditores deben conocer . Auditool.org.* https://www.auditool.org/blog/auditoria-de-ti/6326-5-marcos-de-ciberseguridad-que-los-auditores-deben-conoce
12. Vanegas-Garzón, JH (2017). *Guía de auditoría basada en el análisis de riesgos a un centro de datos aplicando la metodología Magerit 3* . Facultad de Ingeniería.

13. de La Guía Pmbok Sexta Edición Para Obras de, EUMPDEGDEPBENLAT (s / f). *PROYECTO DE TRABAJO DE GRADO* . Edu.co. Recuperado el 14 de diciembre de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/23882/1/PROYECTO%20-%20551344.pdf
14. *GUÍA DE AUDITORÍA PARA EVALUAR EL ASEGURAMIENTO DE LA DISPONIBILIDAD DE LA INFORMACIÓN EN UN AMBIENTE CLOUD COMPUTING IAAS, BAJO LA NORMA ISO 27001 DE 2013* . Edu.co. Recuperado el 14 de diciembre de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/1751/1/TRABAJO%20GRADO%20CLOUD%20COMPUTING%20IAAS.pdf
15. Edu.co. Recuperado el 14 de diciembre de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/25731/1/Trabajo%20de%20Grado_Eliana_robayo_Gu%2b%c2%a1a%20de%20principios_28-11-2020.pdf
16. *ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002* . (s / f). Normas ISO. Recuperado el 15 de diciembre de 2021, de https://www.normas-iso.com/iso-27001/
17. IsecT Ltd. www. isect.com. (s / f). *Marcos de seguridad cibernética ISO / IEC 27110* . Iso27001security.com. Recuperado el 15 de diciembre de 2021, de https://www.iso27001security.com/html/27110.html
18. IsecT Ltd. www. isect.com. (s / f). *Norma de certificación ISO / IEC 27001* . Iso27001security.com. Recuperado el 15 de diciembre de 2021, de https://www.iso27001security.com/html/27001.html
19. IsecT Ltd. www. isect.com. (s / f). *Descripción general de la ciberseguridad ISO / IEC TS 27100* . Iso27001security.com. Recuperado el 15 de diciembre de 2021, de https://www.iso27001security.com/html/27100.html
20. nor27cyg. (s / f). *Guía Implementación ISO 27001 archivos* . ISO 27001. Recuperado el 15 de diciembre de 2021, de https://normaiso27001.es/guia-implementacion-iso-27001
21. Edu.co. Recuperado el 15 de diciembre de 2021, de https://repository.ucatolica.edu.co/bitstream/10983/25345/1/GUIA%20PARA%20ELABORAR%20LA%20%20INFORMACION%20DOCUMENTADA%20PARA%20UN%20SISTEMA%20DE % 20GESTION% 20DE% 20CALIDAD% 20BASADO% 20EN% 20LA% 20NTC% 20ISO% 209001-2015% 20PARA% 20LA% 20EMPRESA% 20B% 20% 26% 20Z% 20INGENIERIA% 20SAS..pdf
22. *Modelo de Seguridad* . (s / f). Recuperado el 15 de diciembre de 2021, de https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
23. *Implementación de un Marco de Ciberseguridad ISO 27032* . (s / f). Isecauditors.com. Recuperado el 15 de diciembre de 2021, de https://www.isecauditors.com/consultoria-csf-iso-27032
24. *Ciberseguridad utilizando la norma ISO 27032: 2012* . (s / f). Sisteseg.com. Recuperado el 15 de diciembre de 2021, de https://sisteseg.com/blog/wp-content/uploads/2018/12/ISO-27032-v-2.pdf

25. (S / f). Nqa.com. Recuperado el 15 de diciembre de 2021, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion .pdf
26. IsecT Ltd. www. isect.com. (s / f). *ISO / IEC 27010 Gestión de la seguridad de la información para comunicaciones intersectoriales* . Iso27001security.com. Recuperado el 15 de diciembre de 2021, de https://www.iso27001security.com/html/27010.html
27. Almanzar-Espitia, N. y Vanzina-Solís, JD (2018). *Auditoría al cumplimiento de una política de desarrollo seguro basada en la ISO 27001. Caso de estudio: Escuela Colombiana de Ingeniería Julio Garavito* . Facultad de Ingeniería
28. IsecT Ltd. www. isect.com. (s / f). *Descripción general de la ciberseguridad ISO / IEC TS 27100* . Iso27001security.com. Recuperado el 15 de diciembre de 2021, de https://www.iso27001security.com/html/27100.html
29. Ciberseguridad utilizando la norma ISO 27032:2012. (s/f). Sisteseg.com. Recuperado el 4 de junio de 2022, de https://sisteseg.com/blog/wp-content/uploads/2018/12/ISO-27032-v-2.pdf
30. Framework documents. (2018, febrero 5). NIST. https://www.nist.gov/cyberframework/framework
31. SEGURIDAD DE LA INFORMACION ISO 27003 v2. (s/f). Nanopdf.Com. Recuperado el 4 de junio de 2022, de https://nanopdf.com/download/seguridad-de-la-informacion-iso-27003-v2_pdf
32. (S/f-a). Greycastlesecurity.com. Recuperado el 4 de junio de 2022, de https://greycastlesecurity.com/wp-content/uploads/2022/03/gcs-iso27002.pdf
33. (S/f-b). Nqa.com. Recuperado el 4 de junio de 2022, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf
34. (S/f-c). Nqa.com. Recuperado el 4 de junio de 2022, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27002-Mapping-ES.pdf