UNIVERSIDAD INTERNACIONAL SEK

DIGITAL SCHOOL

TRABAJO DE FIN DE CARRERA

TITULADO:

MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA DE FABRICACIÓN, COMERCIALIZACIÓN Y EXPORTACIÓN DE MUEBLES

Realizado por:
Ing. Marco Vinicio Cedeño Gómez

Directora del proyecto:
Ing. Verónica Rodríguez Arboleda, MBA.

Como requisito para la obtención del título de:
MAGISTER EN CIBERSEGURIDAD

QUITO, marzo 2022

DECLARACIÓN JURAMENTADA

Yo, MARCO VINICIO CEDEÑO GÓMEZ, con cédula de identidad 1719259408, declaro bajo juramento, que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado por ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de esta declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Marco Vinicio Cedeño Gómez

C.C: 1719259408

DECLARATORIA

El presente trabajo de investigación titulado:

"**MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA DE FABRICACIÓN, COMERCIALIZACIÓN Y EXPORTACIÓN DE MUEBLES**"

Realizado por:

MARCO VINICIO CEDEÑO GÓMEZ

Como requisito para la Obtención del Título de:

MÁSTER EN CIBERSEGURIDAD

Ha sido dirigido por la profesora:

ING. VERÓNICA RODRÍGUEZ ARBOLEDA, MBA

Quien considera que constituye un trabajo original de su autor

Ing. Verónica Rodríguez Arboleda, MBA.

DIRECTORA

PROFESORES INFORMANTES

Después de revisar el trabajo presentado, lo ha calificado como apto para su defensa oral ante el tribunal examinador.

Ing. José Luis Medina, MSc.	Ing. Galo Cárdenas, MSc.

Quito, marzo de 2022

DEDICATORIA

Dedico este trabajo a mi esposa Dayana y mis hijas Monserrath y Maité, son el motor que me empuja a superarme cada día.

Marco.

AGRADECIMIENTO

A mi familia por el apoyo brindado durante este período de preparación.

A la Maestría en Ciberseguridad de la Universidad Internacional SEK, por darme la oportunidad de crecer profesionalmente; a todos los profesores que compartieron su conocimiento y vivencias con nosotros los estudiantes.

A mi tutora Ingeniera Verónica Rodríguez, por su guía para desarrollar este trabajo y su apoyo para culminarlo con éxito.

A la compañía de fabricación de muebles, por abrirme las puertas y permitirme aplicar mis conocimientos en su institución.

RESUMEN

El presente proyecto busca establecer un marco de referencia para la implementación de controles de seguridad informática en una empresa de fabricación, comercialización y exportación de muebles, dicho marco de referencia comienza a construirse desde el análisis de los antecedentes en términos de seguridad informática de la organización, de este análisis, se determina que no se puede garantizar que las pocas medidas de seguridad tomadas en la compañía cubran a todos los activos que debería proteger y peor aún se encuentren articulados entre ellos, esto implica que es necesario implementar los controles dictados por algún estándar de la industria, en este caso, se eligió la norma CIS versión 8 debido a que esta sugiere determinados puntos de control para pequeñas empresas que se encuentran en una etapa temprana de implementación de controles de seguridad informática. El desarrollo del marco de referencia busca proveer a la organización pautas claras a seguir al momento de implementar algún control de CIS versión 8 y de esta manera pueda gestionar en un futuro su ciberseguridad con formalidad.

Palabras clave: Marco de referencia, ciberseguridad, CIS v8, IG1, empresa de muebles.

ABSTRACT

The present document establish a framework for the implementation of computer security controls in a furniture manufacturing, marketing and export company, this reference framework begins to be built from the analysis of the background computer security of the organization, this analysis determined that it cannot be guaranteed that the few security measures taken in the company cover all assets, this implies that it is necessary to implement the controls dictated by some industry standard, CIS version 8 was chosen in this case because it suggests certain checkpoints for small businesses that are at an early stage of implementing computer security controls. The development of the framework seeks to provide the organization with clear guidelines to follow when implementing any CIS version 8 control and in this way it can formally manage its cybersecurity in the future.

Keywords: Framework, cybersecurity, CIS v8, IG1, furniture factory.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I

INTRODUCCIÓN

1 El problema de investigación

1.1 Planteamiento del problema

La digitalización de los procesos en las organizaciones abre la puerta a nuevos riesgos en cuanto a la seguridad cibernética se refiere, esto obliga a las empresas a invertir en soluciones tecnológicas de protección digital y en recursos profesionales para crear y gestionar políticas de seguridad informática y herramientas de ciberseguridad, sin embargo, no todas las organizaciones pueden destinar los recursos económicos suficientes para cubrirse ante las amenazas digitales, adicionalmente el confinamiento mundial ocasionado por la enfermedad de COVID-19, ocasionó en la mayor parte de casos que la transformación digital se diera de manera inesperada y brusca, de un momento a otro nació la necesidad por parte de la gente de contar con los equipos tecnológicos para realizar teletrabajo, estas situaciones aumentan la probabilidad de ser víctima de un delito informático.

La enfermedad de COVID-19 obligó a muchas organizaciones a cambiar varios procesos digitales e implementar nuevos, como es el caso de la empresa dedicada a la fabricación, comercialización y exportación de muebles, durante el confinamiento obligatorio de 2020, la prioridad en la organización fue implementar soluciones informáticas que permitan continuar con el negocio, pasando por alto en muchos casos las normas de seguridad de sus procesos informáticos.

Por ejemplo, los procesos de venta, debieron ser modificados para darle continuidad al negocio, sin embargo, en lo que se refiere a ciberseguridad no se tomó ninguna medida, debido a que la compañía no ha aplicado controles de ciberseguridad porque no cuenta con el conocimiento y equipo humano adecuado para la implementación de estos, esto ocasiona que el personal de la organización se encuentre aún más expuesto a riesgos que amenacen la confidencialidad, integridad y disponibilidad de la información de la empresa, riesgos tales como: fuga o robo de información, daño o robo de equipos, entre otros.

La enfermedad de COVID-19 también ocasionó que, de un día a otro, los usuarios se encuentren fuera de la infraestructura tecnológica que les otorgaba cierto grado de seguridad, esto provocó el aumento de la probabilidad de sufrir algún ataque cibernético, como, por ejemplo: ataques de ingeniería social mediante correo electrónico o redes sociales, infección de los computadores personales con malware por la instalación de software de orígenes desconocidos o por el acceso a sitios web fraudulentos.

1.2 Formulación del problema

En la actualidad, a pesar de que los procesos del giro de negocio han regresado prácticamente a la normalidad, la aplicación de controles de seguridad informática continúa sin implementarse en la empresa dedicada a la fabricación, comercialización y exportación de muebles, esto causa que sea altamente vulnerable ante cualquier tipo de ataque cibernético, debido a que no se puede asegurar que todos los activos de hardware y software pertenecientes a la organización se encuentran debidamente identificados y al no tener actualizado el inventario de estos, cualquier medida de ciberseguridad que se ejecute quedaría incompleta, pues no se puede garantizar que todos los activos han sido considerados en dichas medidas, esto implica la existencia de vulnerabilidades no

cubiertas que podría afectar a la confidencialidad, integridad y disponibilidad de la información.

1.3 Objetivos

1.3.1. Objetivo general

Desarrollar un marco de referencia de ciberseguridad basado en estándares reconocidos de la industria, para la aplicación de controles de seguridad al tratamiento de información de los procesos manejados dentro de la empresa de fabricación, comercialización y exportación de muebles, con la finalidad de protegerla ante cualquier amenaza informática en cualquier momento o en un nuevo confinamiento.

1.3.2. Objetivos específicos

- Analizar las normas de seguridad vigentes para que el marco de referencia se encuentre acorde a los lineamientos dictados por los estándares reconocidos de la industria.
- Evaluar el estado actual de la ciberseguridad en la empresa, mediante el análisis de las medidas de seguridad informática existentes en la misma, para el establecimiento de un escenario previo que aporte al desarrollo del marco de referencia.
- Desarrollar el marco de referencia, basado en los lineamientos de los estándares reconocidos de la industria, para la aplicación de controles de seguridad que permitan la protección de la información de la empresa ante cualquier amenaza informática.
- Definir las fases de implementación del marco de referencia para el inicio de su aplicación en la empresa de fabricación, comercialización y exportación de muebles mediante la ejecución de los controles de inventario y monitoreo de activos de hardware y software.

1.4 Justificación

El mundo se encuentra cursando el proceso llamado democratización del acceso a Internet, esto significa que conforme pasa el tiempo es más sencillo que las personas tengan acceso al mundo digital, y nuestro país no es la excepción. Hoy en día la gente se encuentra hiperconectada, ya sea mediante sus computadores o sus dispositivos móviles, la presencia digital es prácticamente de 24 horas, no importa si se encuentran en su lugar de trabajo o en su hogar, las personas permanentemente se encuentran conectadas a la web.

Si las personas se encuentran hiperconectadas es lógico que las organizaciones también lo estén, esto implica que las instituciones corren los mismos riesgos que cualquier persona en Internet, porque detrás de todo proceso digital dentro de una empresa, siempre se encontrará una persona. Tarde o temprano las organizaciones entienden los riesgos y buscan protegerse, crean políticas de seguridad de la información, implementan herramientas digitales que protejan la infraestructura tecnológica y capacitan a su personal, todo esto genera una sensación de protección.

Por otro lado, ninguna medida de ciberseguridad es infalible, es aquí donde radica la importancia de implementar controles de seguridad informática, y hoy en día más que nunca, debido a que son más frecuentes las noticias de instituciones víctimas de ataques cibernéticos en el territorio ecuatoriano.

Según los datos estadísticos de los últimos cinco años (Tabla 1), levantados por la Fiscalía General del Estado, muestran que más del 90% de las denuncias sobre presuntos delitos informáticos son casos de: suplantación de identidad (66%), apropiación fraudulenta por medios electrónicos (22%) y acceso no consentido a un sistema informático (3.50%), esto implica que los ciberdelincuentes centran sus esfuerzos en

sustraer información confidencial como credenciales de acceso o información personal de sus víctimas.

Tabla 1
Número de denuncias sobre presuntos delitos informáticos, por año de registro y tipo penal. Periodo 01/01/2015 - 31/10/2020

Presunto delito	Ene-Dic 2015	Ene-Dic 2016	Ene-Dic 2017	Ene-Dic 2018	Ene-Dic 2019	Ene-Oct 2020	Total general
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	140	142	216	234	243	259	1.234
Apropiación fraudulenta por medios electrónicos	1.263	1.035	952	1.425	1.709	1.608	7.992
Ataque a la integridad de sistemas informáticos	76	76	84	86	111	79	512
Comercialización ilícita de terminales móviles	1	2	24	13	6	280	326
Contacto con fines sexuales con menores de 18 años por medios digitales	79	102	156	198	163	123	821
Delitos contra la información pública reservada legalmente	5	3	14	12	5	4	43
Interceptación ilegal de datos	55	78	62	40	83	62	380
Oferta de servicios sexuales con menores de 18 años por medios digitales	6	9	11	13	17	4	60
Reemplazo de identificación de terminales móviles	0	5	4	2	0	2	13
Reprogramación o modificación de información de equipos terminales móviles	5	6	7	4	5	4	31
Revelación ilegal de base de datos	23	24	21	43	32	20	163
Suplantación de identidad	3.907	4.132	3.653	4.161	4.575	3.043	23.471
Transferencia electrónica de activo patrimonial	59	45	54	36	46	54	294

Fuente: Sistemas de Actuaciones Fiscales (SIAF)
Elaboración: Dirección de Estadística y Sistemas de Información

Los tres mayores delitos cometidos en el país pueden traer consigo consecuencias tales como: el robo de credenciales de acceso a sistemas informáticos, robo de información, estafas electrónicas o instalación de software malicioso (malware) en los equipos informáticos, todas estas afectan de manera importante a personas y organizaciones, ocasionando pérdidas económicas, ya sea por el robo de dinero, la sustracción o pérdida de información o la imposibilidad de continuidad del negocio, para todo lo mencionado anteriormente, existen formas para defenderse de un ataque o reponerse de uno, sin embargo, no todas las organizaciones le brindan la importancia necesaria a implementar de buena forma su seguridad informática, en este caso, la empresa de fabricación, comercialización y exportación de muebles aunque ya cuenta con ciertas políticas de seguridad informática, estas aún están lejos de posicionarse dentro de la cultura empresarial, debido a esto es importante implementar controles de seguridad informática para reducir los riesgos a los que se encuentran expuestos los activos y la información de la compañía.

1.5 Estado del arte

Noticias sobre ataques informáticos a instituciones públicas o privadas no eran comunes en el país, sin embargo, en los últimos meses se ha vuelto una costumbre amanecer cada cierto tiempo con un nuevo ataque informático a alguna organización.

Como se puede observar en la Figura 1, la suplantación de identidad es el delito informático que permanentemente se encuentra en el primer lugar de denuncias durante los últimos cinco años en el país, mientras más organizaciones sigan migrando sus procesos a Internet, el número de potenciales víctimas de este delito aumenta, si a esto se le suma que por lo general la formación para detectar riesgos en la web es escasa o nula, probablemente con el tiempo los ataques informáticos que tengan éxito aumentarán.

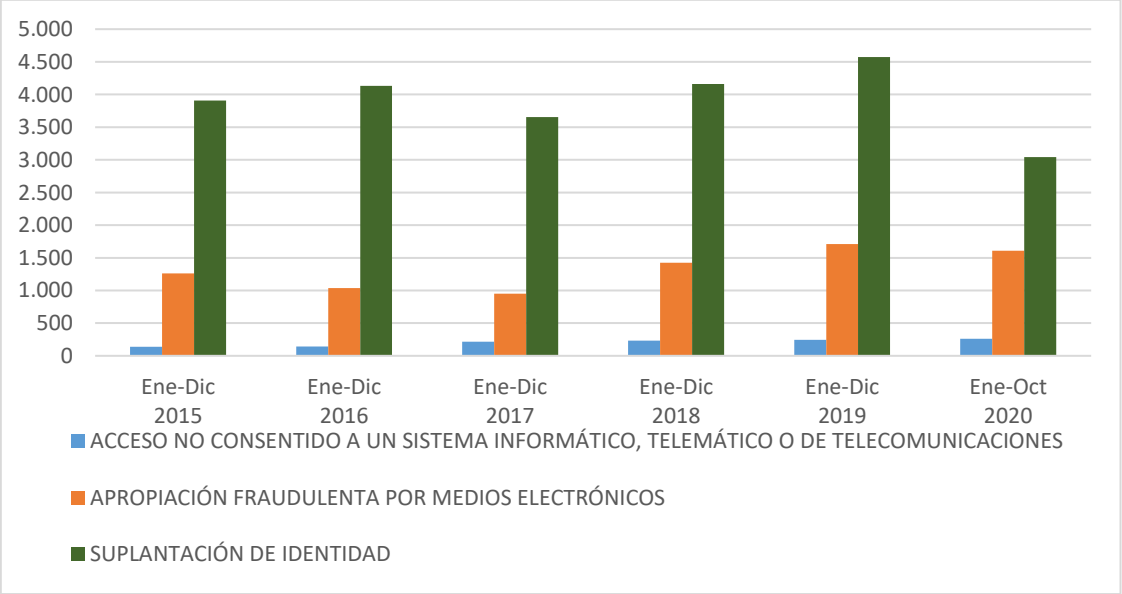

Figura 1 - Gráfica de mayores delitos informáticos en Ecuador, enero 2015 a octubre 2020
Fuente: Sistemas de Actuaciones Fiscales (SIAF)

Los datos mostrados anteriormente no están lejos de la realidad latinoamericana, Cobb, S. (2019) en su artículo: "Guía de Ciberseguridad para Pequeñas Empresas" determina que más del 70% de los ataques están dirigidos a pequeñas y medianas empresas, y dentro de estas, los robos de datos son los ataques más realizados. Al ser pequeñas y medianas las empresas, estas podrían considerar que la información que manejan no tendrá importancia y por ende no serían apetecibles por los ciberdelincuentes, sin embargo, por muy pequeña que se la organización, están tendrá datos sobre clientes, proveedores y la información propia de la empresa, tal como: cuentas, estados financieros y datos personales de sus empleados, todos estos datos tienen un grado de importancia en cuanto a ciberseguridad se refiere.

El artículo de la firma de antivirus Kaspersky (2021). Consejos de ciberseguridad para pequeñas empresas: Aspectos básicos, afirma que en gran medida pequeñas y medianas organizaciones no tiene claro como empezar a proteger su información y la de sus colaboradores (empleados, clientes y proveedores), sin embargo, sugieren al igual que Cobb (2019) algunos pasos a seguir para comenzar a implementar normas de seguridad

informática dentro de una empresa, estos se resumen en analizar los activos con los que cuenta la organización, sus riesgos y amenazas, crear políticas que permitan gestionar la seguridad de la información e infraestructura tecnológica, elegir los controles que permitan aplicar las políticas creadas, implementar los controles que permitan cumplir con las políticas anteriores y por último capacitar y concientizar al personal sobre seguridad.

CAPÍTULO II

MARCO TEÓRICO

2.1. Marco Teórico

El gran reto de los profesionales en ciberseguridad es alcanzar el punto medio entre la protección de la información, los sistemas informáticos y el desempeño eficiente del giro del negocio de la organización, es decir, las medidas para proteger a una empresa de las amenazas cibernéticas no deben interferir con el correcto desempeño de las actividades laborales.

2.1.1. Seguridad de la Información

ISOTools Excellence (2017), define la seguridad de la información como una disciplina que tiene por objetivo implementar de manera técnica la protección de la información, es decir, analiza los riesgos y amenazas, recomienda buenas prácticas y la utilización de las normas de seguridad para asegurar los procesos que busca garantizar la creación, almacenaje, transmisión, utilización, recuperación y disponibilidad de los datos, en otras palabras, la seguridad de la información pretende garantizar la triada (confidencialidad, integridad y disponibilidad) de la seguridad de la información.

2.1.2. Ciberseguridad

Según Newmeyer (2015), Ciberseguridad es el conjunto de políticas de entrenamiento y tecnología diseñadas para proteger el entorno cibernético con el objetivo de asegurar la

confidencialidad, integridad y disponibilidad de la información y la habilidad de conectar dispositivos para que operen según su diseño.

La Ciberseguridad se encuentra abarcada dentro de la Seguridad de la Información, mientras la primera se encarga de tomar acciones de cierto modo ofensivas para proteger la información y los sistemas, la última pretende ser una guía preventiva de riesgos y amenazas que rodean a la información.

2.1.3. Margerit

Según Gutiérrez (2013), "Margerit es una metodología que ofrece un método para analizar los riesgos que traen consigo las tecnologías de la información y permite implementar medidas de control adecuados para mitigar los riesgos". Esta metodología se basa en estudiar el impacto que puede tener en una organización diferentes amenazas que puedan explotar las vulnerabilidades que la empresa presenta, para de estar forma elaborar medidas preventivas y correctivas apegadas a la realidad de la organización. Se recomienda utilizar esta metodología para iniciar la ejecución de un plan de ciberseguridad, debido a que permite centrar la toma de decisiones en los riesgos que pueden tener mayor criticidad.

2.1.4. Análisis de Riesgos

Según Incibe en su artículo web, "¡Fácil y sencillo! Análisis de riesgos en 6 pasos", el cálculo del riesgo puede estar basado en criterios cuantitativos o cualitativos.

En el caso de un análisis cuantitativo se puede otorgar un valor al nivel de probabilidad (Tabla 2) e impacto (Tabla 3) que tendría una amenaza sobre un activo.

Tabla 2
Tabla para el cálculo de la probabilidad

Probabilidad (Cualitativo)	Medida (Cuantitativo)	Descripción
Baja	1	La amenaza ocurre una vez al año
Media	2	La amenaza ocurre una vez al mes.
Alta	3	La amenaza ocurre una vez a la semana.

Fuente: Incibe

Tabla 3
Tabla para el cálculo del impacto

Impacto (Cualitativo)	Medida (Cuantitativo)	Descripción
Bajo	1	El daño ocasionado por la amenaza no tiene consecuencias graves para la organización.
Medio	2	El daño ocasionado por la amenaza tiene consecuencias medianas para la organización.
Alto	3	El daño ocasionado por la amenaza tiene consecuencias muy graves para la organización.

Fuente: Incibe

Una vez determinadas las tablas de probabilidad e impacto de una amenaza, el riesgo se calcula de la multiplicación de la probabilidad por el impacto, es decir:

RIESGO = PROBABILIDAD x IMPACTO.

Aplicando la metodología Margerit se puede obtener las tablas de análisis de riesgos cualitativa y cuantitativa (Tabla 4).

Tabla 4
Tabla de cálculo de riesgo

		PROBABILIDAD		
IMPACTO		Baja (1)	Media (2)	Alta (3)
	Bajo (1)	Bajo (1)	Medio-Bajo (2)	Medio (3)
	Medio (2)	Medio-Bajo (2)	Medio (4)	Medio-Alto (6)
	Alto (3)	Medio (3)	Medio-Alto (6)	Alto (9)

Fuente: Autor

La tabla anterior otorga una escala de evaluación del riesgo, donde, el riesgo evaluado como 1 o 2 será catalogado como bajo, 3 o 4 medio y entre 5 y 9 alto, esto provee una herramienta para catalogar los riesgos y determinar cuáles son los más críticos y prioritarios.

2.1.5. Tratamiento de riesgos

Según Incibe en su documento "Gestión de riesgos, una guía de aproximación para el empresario", una vez determinados los riesgos, se debe decidir qué medidas se tomarán al respecto, es decir, la empresa debe determinar los criterios para establecer si se debe evitar, reducir o mitigar, transferir o aceptar cada uno de los riesgos. En este punto se debe considerar el costo que supondría para la organización hacerse cargo del tratamiento del riesgo, de este modo, si los beneficios son escasos como consecuencia del tratamiento del riesgo se puede optar por evitar el riesgo dejando de realizar algún proceso; si los beneficios se equiparan al costo se puede optar por mitigar el riesgo y si es menos costoso que el tratamiento del riesgo lo realice un tercero se puede optar por transferir el riesgo.

2.1.6. Normativas

Implementar controles de seguridad informática en una organización es una tarea titánica, existen tantos puntos a considerar que sería fácil pasar por alto muchos de los riesgos y amenazas a las que la información y la infraestructura tecnológica están expuestas, debido a estos se han creado normativas que brindan una hoja de ruta y buenas prácticas a las instituciones para establecer medidas de seguridad ante amenazas físicas y digitales. Entre estas normativas se encuentran:

2.1.7. Norma ISO 27001

Según el sitio web dedicado a la Seguridad de la Información isotools.org, "ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan", esta norma permite realizar un análisis de los riesgos y aplicar las medidas necesarias para mitigarlos o eliminarlos.

La norma ISO 27001 en su cuerpo presenta la estructura detallada en la Tabla 5.

Tabla 5
Estructura de la norma ISO-27001

Nº	Etapa	Descripción
1	Objeto de aplicación	Explica el uso, finalidad y modo de aplicación de la norma.
2	Referencias Normativas	Sugiere el estudio de documentos indispensables para su aplicación.
3	Términos y Definiciones	Describe los términos aplicados en la norma.
4	Contexto de la organización	Recopila las necesidades y expectativas internas y externas de la organización, que afecten a la implementación del sistema de gestión de la seguridad de la información.
5	Liderazgo	Busca la contribución de todos los empleados de la organización para la aplicación de la norma, mediante la elaboración de políticas de seguridad, asignación de roles y responsabilidades.
6	Planificación	En esta etapa se debe detectar, analizar y evaluar los riesgos de seguridad de la información y el tratamiento que se darán a estos. En este punto también se establece los objetivos de la seguridad de la información y como conseguirlos.
7	Soporte	Señala que la organización debe contar con los recursos, competencias del personal, toma de conciencia de todos los actores interventores, comunicación dentro de la empresa e información documentada pertinente en cada caso.
8	Operación	Detalla el cómo se debe planificar, implementar y controlar los procesos de la organización, así como la evaluación de los riesgos y su tratamiento.
9	Evaluación de desempeño	Recalca la necesidad de realizar el seguimiento, medición, análisis, evaluación, auditoría interna y revisión del sistema de gestión de la información.

Nº	Etapa	Descripción
10	Mejora	Trata las no conformidades y las acciones correctivas tomadas, adicionalmente la mejora continua del sistema de gestión de seguridad informática.

Fuente: isotools.org
Elaborado por: Autor

Adicional a esto cuenta con 114 controles detallados en su Anexo A, estos se dividen en 14 secciones, que son las siguientes:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Controles de acceso.
- Criptografía – Cifrado y gestión de claves.
- Seguridad física y ambiental.
- Seguridad operacional.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento del sistema.
- Gestión de incidentes de seguridad de la información.
- Cumplimiento.

2.1.8. Norma CIS

El "Center for Internet Security" elaboró esta norma, los Controles de Seguridad Crítica de CIS junta las mejores prácticas en ciberseguridad y sus recomendaciones de defensa buscan evitar daños por ataques informáticos. "Los controles de CIS proporcionan una orientación específica y una vía clara para que las organizaciones alcancen las metas y los objetivos descritos por múltiples marcos jurídicos, reglamentarios y normativos" (Manage Engine, 2021).

En su versión 8 cuenta con 18 controles, estos se encuentran organizados en tres grupos de implementación (IG1, IG2, IG3), dependiendo el tamaño de la organización y su experiencia en ciberseguridad se puede optar por empezar por uno de estos grupos.

- **IG1** – Organizaciones con recursos y poca o nula experiencia en ciberseguridad.
- **IG2 –** Empresas que emplean a personal exclusivamente para administrar y proteger la infraestructura tecnológica.
- **IG3 –** Empresas que emplean personal especializado en ciberseguridad.

Por ejemplo, como se puede observar en la Tabla 6, en el control uno de CIS sus subcontroles se encuentra clasificados en los grupos de implementación en los que se deben aplicar, en este caso, los subcontroles 1.1 y 1.2 deben ser implementados en todos los grupos, mientras tanto, el 1.5 solamente si se selecciona el grupo de implementación tres.

Tabla 6
Ejemplo clasificación contro uno de norma CIS versión 8

Control CIS	Subcontrol CIS	Título	IG1	IG2	IG3
1		Inventario y control de activos empresariales			
1	**1.1**	Establecer y mantener un inventario detallado de activos empresariales	**x**	**x**	**x**
1	**1.2**	Abordar activos no autorizados	**x**	**x**	**x**
1	**1.3**	Utilizar una herramienta de detección activa		**x**	**x**
1	**1.4**	Usar el registro del Protocolo de configuración dinámica de host (DHCP), para acutalizar el inventario de activos empresariales.		**x**	**x**
1	**1.5**	Usar una herramienta de descubrimiento pasivo de activos			**x**

Fuente: cisecurity.org
Elaborador por: Autor

Los 18 controles de CIS en su versión 8 son los siguientes:

- **Control 1 -** Inventario y control de activos de hardware empresariales.
- **Control 2** - Inventario y control de activos de software empresariales.
- **Control 3** - Protección de datos.
- **Control 4 -** Configuración segura de activos y software empresariales.
- **Control 5 -** Gestión de cuentas.
- **Control 6 -** Gestión del control de acceso.
- **Control 7 -** Gestión continua de vulnerabilidades.
- **Control 8 -** Gestión de registros de auditoría.
- **Control 9 -** Protecciones de correo electrónico y navegador web.
- **Control 10 -** Defensas contra software malicioso.
- **Control 11 -** Recuperación de datos.
- **Control 12 -** Gestión de la infraestructura de red.
- **Control 13 –** Supervisión y defensa de la red.
- **Control 14 -** Conciencia de seguridad y capacitación en habilidades.
- **Control 15 -** Gestión de proveedores de servicios.
- **Control 16 –** Seguridad del software de aplicación.
- **Control 17 -** Gestión de respuesta a incidentes.
- **Control 18 –** Pruebas de penetración.

Para CIS, cada empresa debe autoevaluarse y determinar a qué grupo de implementación pertenece, en este caso, basado en el análisis situacional de la empresa de fabricación, comercialización y exportación de muebles, esta se encuentra dentro del grupo de implementación IG1, debido a que cuenta con personal y recursos limitados en

cuanto al manejo de la ciberseguridad, de esta forma los subcontroles a tomar en cuenta son los detallados en la tabla mostrada en el Anexo A.

2.1.8.1. Puntos de Control del Grupo de Implementación Uno (IG1)

Los puntos de control que se considerarían a implementar dentro del desarrollo de este marco de referencia son los detallados en el grupo de implementación IG1 de CIS Versión 8, estos son recomendados para las organizaciones que iniciarán a administrar su ciberseguridad o se encuentran en una etapa temprana de implementación de controles de seguridad.

Los puntos de control del grupo de implementación IG1 son:

- **Control 1** - Inventario y control de activos de hardware empresariales.
- **Control 2** - Inventario y control de activos de software empresariales.
- **Control 3** - Protección de datos.
- **Control 4** - Configuración segura de activos y software empresariales.
- **Control 5** - Gestión de cuentas.
- **Control 6** - Gestión del control de acceso.
- **Control 7** - Gestión continua de vulnerabilidades.
- **Control 8** - Gestión de registros de auditoría.
- **Control 9** - Protecciones de correo electrónico y navegador web.
- **Control 10** - Defensas contra software malicioso.
- **Control 11** - Recuperación de datos.
- **Control 12** - Gestión de la infraestructura de red
- **Control 14** - Conciencia de seguridad y capacitación en habilidades.
- **Control 15** - Gestión de proveedores de servicios.
- **Control 17** - Gestión de respuesta a incidentes.

Cada uno de los puntos detallados anteriormente puede otorgar un valor agregado a la organización, tal como se detalla en la Tabla 7.

Uno de los beneficios de implementar controles de ciberseguridad es el de poder estimar un presupuesto económico para la gestión de la seguridad informática dentro de la organización, esto permitirá destinar recursos para dicha implementación y como consecuencia, al haber un presupuesto predefinido, las autoridades se comprometerán también en su adecuado desarrollo.

Tabla 7

Valor agregado a la organización de los puntos de control IG1

Control CIS	Título	Descripción	Valor agregado
1	Inventario y control de activos empresariales	Administrar de manera activa todos los activos de la empresa conectados a la infraestructura física, virtual, remota y aquellos dentro de entornos de nube, para conocer con precisión la totalidad de los activos que deben monitorearse y protegerse dentro de la empresa. Esto también apoyará la identificación de activos no autorizados y no operados para eliminar o remediar.	• Visualizar todos los activos tecnológicos físicos, permite manejar presupuestos de mantenimiento o renovación de equipos. • Elaborar un plan de mantenimiento de dispositivos para prevenir fallos que afecten al desarrollo de la actividad laboral. • Prevenir el uso incorrecto de los equipos, que puedan afectar a la información o a la vida útil del equipo.
2	Inventario y control de activos de software	Administrar de manera activa todo el software en la red para que solo se instale y pueda ejecutarse el software autorizado, e impedir la instalación o ejecución de software no autorizado.	• Conocer todos los activos tecnológicos de software permite la elaboración de un presupuesto de licencias de estos. • Mantener un listado actualizado del software utilizado dentro de la organización, permitirá establecer planes de actualización de estos. • Mantener un listado actualizado del software utilizado permite desarrollar planes de capacitación al personal del uso software, lo que otorga un crecimiento profesional que puede mejorar la productividad.
3	Protección de datos	Desarrollar procesos y controles para identificar, clasificar, manejar, retener y eliminar datos de forma segura.	• Establecer el correcto manejo de la información dentro de la organización puede prevenir problemas del tipo legal a la organización. • Clasificar la información otorgará de manera más clara y transparente la responsabilidad de cada persona sobre dicha información.
4	Configuración segura de activos y software empresariales	Crear y gestionar la configuración segura de los activos empresariales y software.	• Establecer configuraciones correctas permite evitar ataques cibernéticos que traen como consecuencias grandes pérdidas económicas.
5	Gestión de cuentas	Utilizar procesos y herramientas para asignar y administrar la autorización de credenciales para cuentas de usuario, incluidas cuentas de administrador, así como cuentas de servicio, para activos y software empresariales.	• Permite otorgar responsabilidades claras a cada uno de los roles dentro de la organización, agiliza el desarrollo de los procesos organizacionales.

Control CIS	Título	Descripción	Valor agregado
6	Gestión del control de acceso	Usar procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos y software empresariales.	• Permite otorgar responsabilidades claras a cada uno de los roles dentro de la organización, agiliza el desarrollo de los procesos organizacionales. • Permite controlar el uso de equipos y software por parte del personal, lo que otorga medidas para prevenir la subutilización de algún activo.
7	Gestión continua de vulnerabilidades	Desarrollar un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos empresariales dentro de la infraestructura de la empresa, con el fin de remediar y minimizar oportunidades para los atacantes.	• Permite evitar ataques cibernéticos que pueden tener como consecuencias grandes pérdidas económicas.
8	Gestión de registros de auditoría	Recopilar, alerte, revise y conserve registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.	• Permite responder a ataques cibernéticos que pueden tener como consecuencias grandes pérdidas económicas.
9	Protecciones de correo electrónico y navegador web	Mejorar las defensas y detecciones de amenazas del correo electrónico y los vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través de la participación directa.	• Permite evitar y/o responder a ataques cibernéticos que pueden tener como consecuencias grandes pérdidas económicas o el compromiso de la seguridad de información sensible.
10	Defensas contra software malicioso	Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, código o scripts malintencionados en activos empresariales.	• Permite evitar ataques cibernéticos que pueden tener como consecuencias grandes pérdidas económicas.
11	Recuperación de datos	Crear y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales dentro del ámbito a un estado previo al incidente y de confianza.	• Permite recuperarse de un atentando a la confiabilidad, integridad y disponibilidad de la información, permitiendo reducir el impacto económico ocasionado por dicho atentado.
12	Gestión de la infraestructura de red	Crear, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, para evitar que los atacantes exploten los servicios de red y puntos de acceso vulnerables.	• Permite evitar ataques cibernéticos que pueden tener como consecuencias grandes pérdidas económicas.
14	Conciencia de seguridad y	Crear y gestionar un programa de concientización de seguridad para influir en el comportamiento entre la fuerza laboral para que sea consciente de la seguridad y	• Capacitar y entrenar al personal permite contar con personas preventivas que puedan anticipar algún tipo de ataque permite minimizar las superficies de ataques, lo que se puede traducir

Control CIS	Título	Descripción	Valor agregado
	capacitación en habilidades	esté debidamente capacitado para reducir los riesgos de ciberseguridad para la empresa.	en un mejor uso de los presupuestos destinados a ciberseguridad.
15	Gestión de proveedores de servicios	Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales, o son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.	• Blinda a la organización ante acciones legales, otorgando responsabilidades de seguridad a los proveedores. • Promueve la aplicación de buenas prácticas a otras organizaciones, lo que genera la expansión de un ambiente interinstitucional más seguro. • Permite recuperarse de un atentando a la confiabilidad, integridad y disponibilidad de la información, permitiendo reducir el impacto económico ocasionado por dicho atentado.
17	Gestión de respuesta a incidentes	Crear un programa para desarrollar y mantener una capacidad de respuesta a incidentes para preparar, detectar y responder rápidamente a un ataque.	• Permite recuperarse de un atentando a la confiabilidad, integridad y disponibilidad de la información, permitiendo reducir el impacto económico ocasionado por dicho atentado.

Fuente: Auto

2.1.9. Normativa NIST

NIST, National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología), pretende ser una guía de implementación de planes de ciberseguridad para todo tipo de negocio independientemente de su tamaño, NIST tiene como objetivo que las organizaciones puedan comprender mejor sus riesgos de ciberseguridad, administrarlos y reducirlos y proteger sus redes y datos.

Esta normativa se basa en cinco fases, que son las siguientes:

- **Identificar –** Busca determinar el contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos de las personas, activos e información relacionados con la ciberseguridad para centrar y priorizar esfuerzos, de acuerdo con su estrategia de administración de riesgos y las necesidades comerciales.
- **Proteger -** Permite establecer las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras tecnológicas críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.
- **Detectar -** Busca identificar la ocurrencia de un evento de ciberseguridad mediante la monitorización continua, permitiendo el descubrimiento oportuno de los mismos.
- **Responder –** Define las actividades necesarias para tomar medidas frente a un incidente de ciberseguridad detectado para mitigar su impacto.

- **Recuperar –** Busca establecer el despliegue de actividades para la gestión de resiliencia y el retorno de las operaciones normales después de un incidente reduciendo su impacto.

La normativa NIST cuenta con 20 controles resumidos en la Tabla 8.

Tabla 8
Controles normativa NIST

Número	Control	Objetivo
CS1	Inventario de dispositivos autorizados y no autorizados	Gestionar activamente todos los dispositivos hardware en la red, solo los dispositivos autorizados deben tener acceso a la red.
CS2	Inventario de software autorizado y no autorizado	Gestionar activamente todo el software, de forma que solo se pueda instalar y ejecutar software autorizado.
CS3	Configuraciones seguras de software y hardware para dispositivos móviles, portátiles, equipos de escritorio y servidores	Establecer una configuración segura para dispositivos móviles, portátiles, equipos de escritorio y servidores, gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los ataques.
CS4	Proceso continuo de identificación y remediación de vulnerabilidades	Disponer un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.
CS5	Control sobre privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.
CS6	Mantenimiento, monitorización y análisis de logs de auditoría	Recoger, gestionar y analizar registros de auditoría de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.
CS7	Protección del correo electrónico y del navegador	Minimizar la posibilidad de que los atacantes manipulen a los empleados a través de su interacción con el correo electrónico y el navegador.
CS8	Defensas contra el malware avanzado de correo electrónico y del navegador	Evitar la instalación, difusión y ejecución de código malicioso en distintos puntos.
CS9	Limitar y controlar los puertos de red, protocolos y servicios	Gestionar el uso de puertos, protocolos y servicios en los dispositivos que tengan red para reducir las vulnerabilidades disponibles a los atacantes.

Número	Control	Objetivo
CS10	Capacidad de recuperación de datos	Disponer procesos, metodologías y herramientas adecuadas para respaldar la información crítica y realizar pruebas de recuperación.
CS11	Configuraciones seguras de dispositivos de red (firewalls, routers y switches)	Establecer una configuración base para los dispositivos de infraestructura de red, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso.
CS12	Defensa perimetral	Desarrollar una estrategia para detectar, prevenir y corregir los flujos de transmisión de información entre redes de distintos niveles de seguridad (confianza).
CS13	Protección de los datos	Disponer de procesos y herramientas adecuadas para prevenir la fuga de información, mitigar los efectos cuando se ha producido un incidente de fuga de información, y asegurar la confidencialidad e integridad de la información sensible.
CS14	Acceso basado en la necesidad de conocer (need to know)	El acceso a los activos críticos debe realizarse de acuerdo con una definición formal de que personas, sistemas y aplicaciones tienen la necesidad y el derecho de acceso.
CS15	Control de acceso wireless	Disponer de procesos y herramientas para garantizar una seguridad adecuada en las redes Wifi y en los sistemas clientes, incluyendo seguimiento y corrección de las medidas de seguridad.
CS16	Control y monitorización de cuentas de sistema	Gestionar activamente el ciclo de vida de las cuentas de sistema y de aplicación (creación, uso, inactividad y borrado).
CS17	Verificación de las habilidades de seguridad y formación adecuada	Identificar los conocimientos específicos, habilidades y capacidades necesarias en la organización para la defensa de los activos críticos de la compañía, y desarrollar y evaluar un plan para identificar gaps y remediar con políticas, formación y programas de sensibilización.
CS18	Seguridad en el ciclo de vida de las aplicaciones	Gestionar el ciclo de vida de todas las aplicaciones, tanto las desarrolladas internamente como las de proveedores para prevenir, detectar y corregir vulnerabilidades técnicas.
CS19	Gestión y respuesta a incidentes	Proteger la información y la reputación de la organización desarrollando e implementando una infraestructura de respuesta a incidentes para detectar un ataque, contener el daño de forma efectiva, expulsar al atacante, y restaurar la integridad de los sistemas y la red.

Número	Control	Objetivo
CS20	Realizar test de penetración y ejercicios de ataque	Probar las defensas de la organización (tecnología, procesos y personas) mediante la simulación de un ataque, utilizando sus mismas acciones y objetivos.

Fuente: netsecurechile.wordpress.com

Según la capacidad económica y humana o según los objetivos que la organización tenga para su programa de ciberseguridad se puede optar por una u otra normativa.

Todas las normativas tienen como objetivo brindar una guía a las organizaciones para poder implementar sus programas de seguridad cibernética y prácticamente se basan en grosso modo en los siguientes puntos: identificar los activos además de los riesgos y amenazas a los que se encuentran expuestos, proteger dichos activos, monitorear y responder ante ataques, y por último recuperar la información o sistemas afectados.

NIST también cuenta con una publicación especial, NIST 800-50, en la que detalla una guía para la construcción de un programa de entrenamiento y habilidades de seguridad en las tecnologías de la información, esta guía se basa en tres componentes detallados en la Tabla 9.

Tabla 9
Fases de programa de entrenamiento NIST 800-50

COMPONENTE	DESCRIPCIÓN
Concienciación	La conciencia no es entrenamiento, su propósito es que los individuos reconozcan la importancia de la ciberseguridad.
Entrenamiento	El entrenamiento se centra en producir habilidades de seguridad necesarias.
Educación	La educación integra todas las habilidades de seguridad desarrolladas y se esfuerza en crear profesionales con visión y respuesta proactiva.

Fuente: Publicación especial NIST 800-50

Como se puede observar NIST cuenta con un amplio catálogo de publicaciones que promueven la aplicación de medidas de seguridad en las organizaciones.

2.2. Marco Conceptual

Incibe (2017), en su documento “Glosario de términos de ciberseguridad” detalla las siguientes definiciones:

2.2.1. Confidencialidad

Refiere a que la información de una empresa solo debe ser accesible a él o los usuarios autorizados.

2.2.2. Integridad

La transformación de los datos solamente debe ser realizada por procesos legítimos, durante un período de tiempo y desde un sitio autorizado, para garantizar que la información se encuentre libre de alteraciones y errores accidentales o intencionales.

2.2.3. Disponibilidad

La información sensible de la organización será accesible por el personal autorizado en el momento que se considere necesario.

2.2.4. Activos

Son los recursos de información o sistemas necesarios que permite a una empresa funcionar, si se llegan a comprometer, la organización sufrirá consecuencias negativas.

2.2.5. Vulnerabilidad

Es una debilidad o falla en un sistema que puede permitir que un atacante comprometa la integridad, disponibilidad o confidencialidad de los datos. Estos fallos pueden tener distintos orígenes que pueden pasar por el diseño, configuración o carencias de procedimientos de un sistema.

2.2.6. Amenaza

Son las acciones que pretenden explotar una vulnerabilidad de un sistema para obtener algún tipo de beneficio no legal para quien la ejecuta. Las amenazas pueden provenir desde el exterior o interior de una organización.

2.2.7. Riesgo

Posibilidad de que una vulnerabilidad sea explotada por algún tipo de amenaza, lo que ocasionará el daño parcial o total de la información o de un sistema.

CAPÍTULO III

ANÁLISIS SITUACIONAL

La empresa de fabricación, comercialización y exportación de muebles es una organización ecuatoriana, constituida en el año de 1996, actualmente opera desde su matriz de producción en la ciudad de Quito, y cuenta con sucursales de venta en Quito y Guayaquil, al ser una empresa exportadora forma parte de BASC (Business Alliance for Secure Commerce).

3.1. BASC

Business Alliance for Secure Commerce (BASC), es una alianza empresarial internacional que pretende promover el comercio seguro en cooperación con estados y organismos internacionales, en esta organización pueden participar empresas de todo el mundo que busquen fortalecer el comercio internacional mediante la aplicación de estándares y procedimientos de seguridad avalados por entidades internacionales.

Esta alianza empresarial dispone una norma para la implementación del Sistema de Gestión en Control y Seguridad (SGCS BASC), con la cual las empresas aplicarán una metodología enfocada en procesos, gestión de riesgos y mejora continua. Adicionalmente, los Estándares Internacionales de Seguridad BASC, constituyen un marco para el establecimiento de controles operacionales alineados con el alcance de las empresas, en la cadena de suministro (BASC, 2019).

La norma internacional SGSC BASC puede usarse con otras normativas, a las cuales hace referencia, en cuanto a la seguridad de la información esta se basa en la norma ISO 27001 (Especificaciones para la seguridad de los sistemas de la Información).

3.2. Organigrama

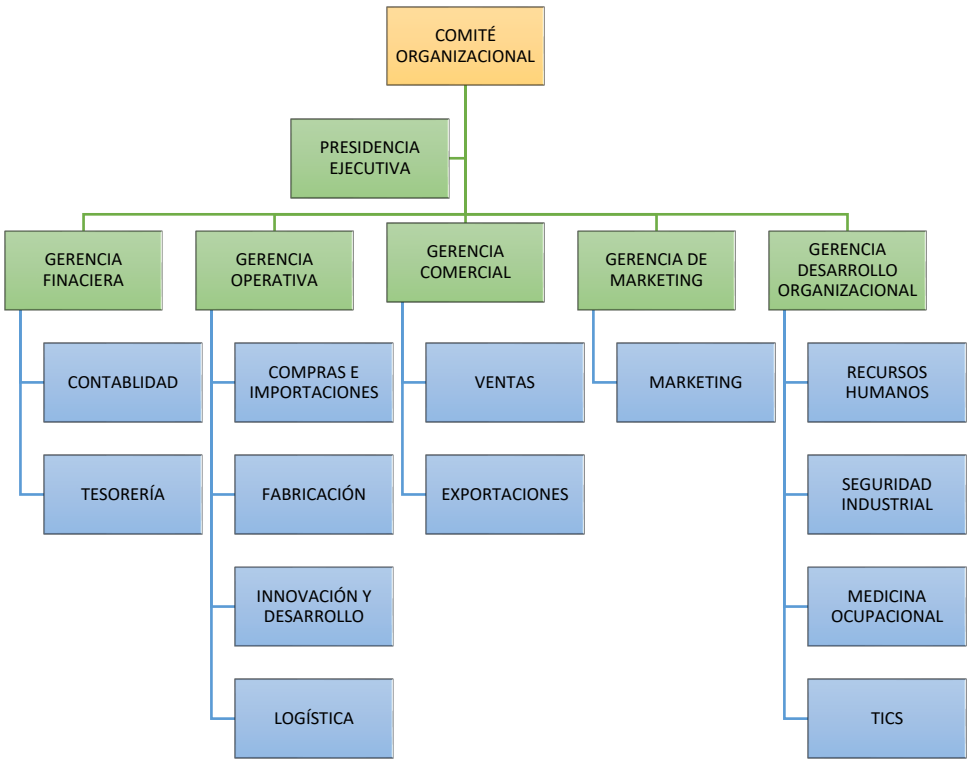

Figura 2 - Organigrama institucional
Fuente: Empresa

La organización cuenta con las siguientes áreas: financiera, de operaciones, comercial, marketing y desarrollo organizacional; dentro de esta última se encuentra el departamento de TICS, cuyas funciones principales son las de soporte técnico, gestión de sistemas y desarrollo de software, las funciones de seguridad informática son realizadas esporádicamente por este departamento.

Como se puede observar en la Figura 2, la empresa de fabricación, comercialización y exportación de muebles no cuenta con un área especialmente de dedicada a la ciberseguridad y mucho menos a la seguridad de la información, sin embargo, es posible

su creación, debido a que la organización se encuentra iniciando un proceso de crecimiento, planificado a los próximos cinco años.

3.3. Infraestructura

La empresa en su matriz tiene para sus 45 usuarios administrativos una red segmentada en dos subredes protegidas por un sistema de Firewall, esto permite crear reglas de acceso a las distintas redes locales de la organización, una Red MÓVIL a la que se conecta los dispositivos móviles de los empleados y visitantes, y una Red LAN a la que se conectan los computadores de los trabajadores, sólo se permite la conexión a esta última red a los equipos que se dan de alta en el Firewall; por otro lado, la compañía posee una red abierta (Red SIS) que no pasa por el firewall y tiene salida directa a Internet, esta última red es utilizada solo por el departamento de sistemas de la empresa.

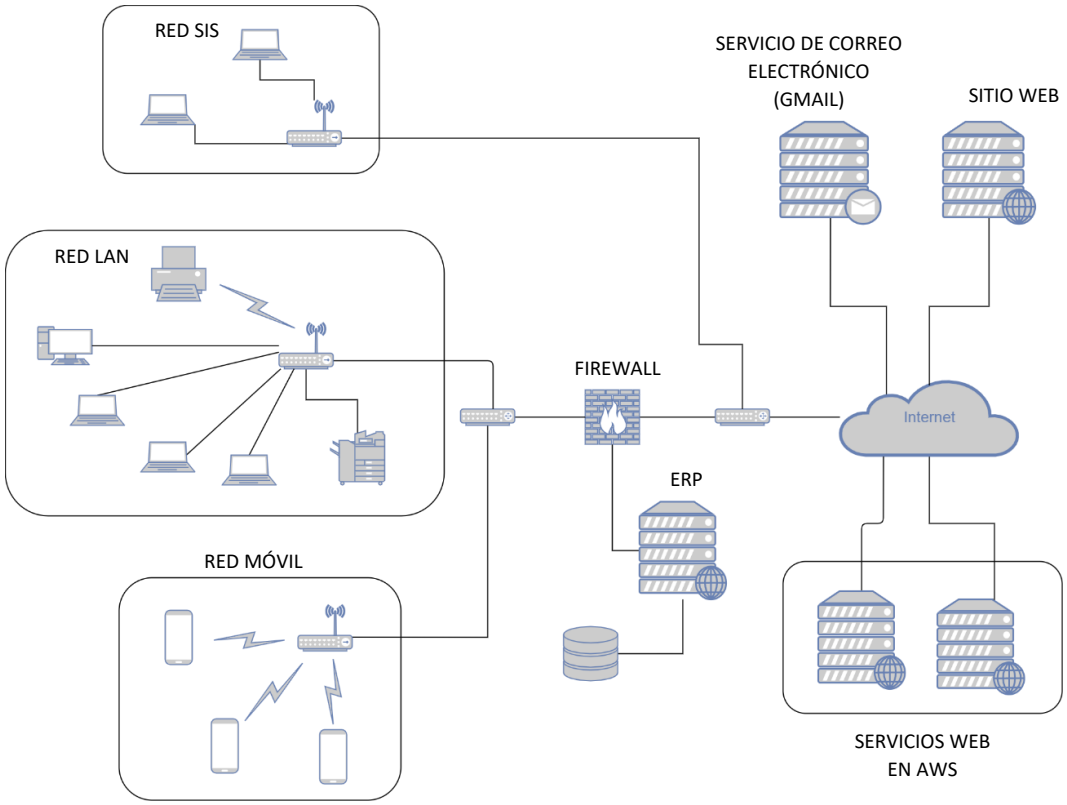

Figura 3 – Arquitectura de red de la empresa
Fuente: Autor

Dentro de la infraestructura de la organización se encuentra conectado el servidor que contiene el sistema ERP corporativa, este se encuentra protegido por el Firewall, su

acceso está permitido tanto desde dentro de la Red LAN como desde internet mediante la IP pública del router del proveedor del servicio de Internet.

Adicional a esto, la organización cuenta con servicios alojados en la nube, tales como: el servicio de correo electrónico alojado en el servicio de Gmail, su sitio web establecido en un servicio de hosting, adicionalmente dos sistemas de uso corporativo implementados en máquinas virtuales dentro de la infraestructura AWS. En la Figura 3, se puede observar la arquitectura detalla en los párrafos anteriores.

3.4. Políticas Existentes

Debido a que la empresa posee la certificación BASC (detallada en el punto 3.1 de este documento), está obligada a gestionar la seguridad informática dentro de la organización, por esto, la empresa cuenta al momento con cinco políticas de seguridad detalladas a continuación:

- **PR-122A - Respaldo y recuperación de información**

Más que una política, este documento indica el procedimiento para el respaldo de información tanto de bases de datos, como información de los computadores del personal crítico de la organización.

- **PO-122B - Política de contraseñas de sistemas informáticos**

Establece las normas para la generación y gestión de contraseñas de los usuarios.

- **PO-122C - Política de navegación en internet**

Establece ciertos lineamientos que los usuarios deben seguir al utilizar internet, como la prohibición de acceder a sitios de streaming, o descargar videos de alta definición.

- **PO-122D - Política de Uso de Equipos de Informáticos.**

Establece ciertas recomendaciones para los usuarios del uso de los equipos informáticos como los cuidados básicos y las responsabilidades del departamento de sistemas al otorgar un equipo a un nuevo usuario.

- **PO-122E - Política de Firmas en Correo Electrónico**

Establece los lineamientos para el uso de la firma en el correo electrónico, esta no es una política de seguridad, es una normativa de identidad corporativa.

3.5. Antecedentes de incidentes de seguridad

Como antecedentes de incidentes de seguridad dentro de la empresa, se cuenta con un solo documento escrito, una prueba de concepto sobre el correo electrónico de una empresa dedicada a la ciberseguridad, esta prueba arrojó que el servicio de correo electrónico de la organización alojado en Gmail es víctima de ataques de phishing, entre 94389 mensajes se detectó 29 incidentes de los cuales el 100% fueron establecidos como ataques de phishing, esta prueba determinó que estos correos electrónicos llegaron a la bandeja de entrada de colaboradores de la organización, lo que significa que a pesar de contar con el servicio de email en Google, este no es infalible a recibir ataques cibernéticos.

A pesar de los datos expuestos en el párrafo anterior, no existe un historial de incidentes de seguridad dentro de la compañía, no se ha encontrado documentación histórica escrita de los sucesos dados en la organización, los pocos casos ocurridos se los ha obtenido mediante entrevistas a los trabajadores antiguos del departamento de sistemas, y estos sucedieron cuando tenían el servicio de correo electrónico alojado dentro de los servidores de la organización, al momento de trasladar el manejo de email al servicio corporativo de Gmail, las incidencias bajaron considerablemente, según lo informado, estos incidentes fueron del tipo phishing.

3.6. Análisis de la institución

El giro de negocio de la organización se basa en la fabricación, comercialización y exportación de muebles, y como toda empresa en la actualidad, hace uso de herramientas informáticas que apoyan a la realización de los procesos productivos, esto implica que posee varios puntos críticos en cuanto a la información que maneja, tal como:

- Información de sus productos actuales y futuros.
- Información de empleados.
- Información de proveedores.
- Información de clientes.
- Inventario.
- Información contable.

Todos estos datos se encuentran distribuidos entre el ERP de la organización y los computadores asignados a los empleados de los diferentes departamentos de la empresa.

A pesar de contar con cierto grado de protección dentro de la infraestructura física de la compañía, esta es útil siempre y cuando los computadores portátiles se encuentren conectados a la Red LAN, sin embargo, todos los empleados tienen la facultad de poder utilizar el computador desde el exterior de las instalaciones, esto expone a los empleados a más amenazas cibernéticas cuando utilizan los equipos fuera de la empresa.

Como ya se mencionó, la empresa cuenta con cinco políticas de seguridad, lo que demuestra que son conscientes de la importancia de medidas de seguridad, claro está que la certificación BASC también exige implementarlas, a pesar de esto, no poseen un plan de las normas de seguridad implementadas o por implementar, se puede decir que las medidas tomadas se las ha tomado de forma arbitraria para cumplir con las exigencias de la entidad certificadora.

Normativas como ISO 27001 o CIS, sugieren como primer paso establecer los activos pertenecientes a la organización, debido a que no se puede proteger lo que no se conoce, en este aspecto la organización tiene un avance al contar con una matriz de activos de hardware llevado en una hoja de cálculo, adicionalmente, este listado no se encuentra actualizado (Tabla 10), en este documento se encuentran equipos asignados a personal que ya no labora en la institución y también dispositivos que ya han sido dados de baja, adicional a esto no cuentan con un inventario de los activos de software de la institución.

En la Tabla 10 se puede observar una muestra de los dispositivos utilizados en las instalaciones de la matriz de la empresa, sin embargo, el documento de los activos de hardware de los locales comerciales se encuentra en las mismas condiciones.

Tabla 10
Inventario Activos Fijos Hardware

ACTIVOS MATRIZ						
No. ARTÍCULO	**RESPONSABLE**	**TIPO**	**MARCA**	**DATOS PC**	**DEPARTAMENTO**	**NOMBRE DE EQUIPO**
IP008	xxxxxx	Ipad	Apple			
IP008	xxxxxx	Ipad	Apple			
C060	xxxxxx	Desktop	Apple	Windows 10 Pro	Marketing	
C057	xxxxxx	Laptop	Dell	Windows 10 Pro	Contabilidad	XXXXXXXXXXXX
C055	xxxxxx	Laptop	HP	Window 10 Home	Tesorería	XXXXXXXXXXXX
C053	xxxxxx	Desktop	HP	Windows 10 Pro	Recursos Humanos	XXXXXXXXXXXX
C051	xxxxxx	Laptop	Lenovo	Windows 10 Pro	Contraloria	XXXXXXXXXXXX
C050	xxxxxx	Laptop	Lenovo	Window 10 Pro	Calidad	XXXXXXXXXXXX
C048	xxxxxx	Laptop	Lenovo	Windows 10 Pro	Comercio Exterior	
C047	xxxxxx	Laptop	dell	Windows 10 Pro	Centro Médico	XXXXXXXXXXXX
C046	xxxxxx	Laptop	HP	Windows 8.1 Pro	Centro Médico	XXXXXXXXXXXX
C045	xxxxxx	Laptop	Apple		Presidencia Ejecutiva	
C044	xxxxxx	Laptop	Dell	Windows 10 Pro	Innovación y Desarrollo	XXXXXXXXXXXX
C058	xxxxxx	Laptop	Lenovo	Windows 10 Pro	Producción	XXXXXXXXXXXX
C038	xxxxxx	Laptop	Lenovo	Windows 10 Home	Gerencia de Negocios Internacionales	XXXXXXXXXXXX

ACTIVOS MATRIZ						
No. ARTÍCULO	**RESPONSABLE**	**TIPO**	**MARCA**	**DATOS PC**	**DEPARTAMENTO**	**NOMBRE DE EQUIPO**
C037	xxxxxx	Laptop	DELL	Windows 10 Pro	Comex	XXXXXXXXXXXX
C036	xxxxxx	Laptop	Dell	Windows 10 Pro	Contabilidad	XXXXXXXXXXXX
C034	xxxxxx	Laptop	Lenovo	Windows 10 home	Recursos Humanos	XXXXXXXXXXXX
C033	xxxxxx	Laptop	Dell	Windows 10 Pro	Producción	XXXXXXXXXXXX
C031	xxxxxx	Desktop	ASUS-Intel	Windows 7 Professional	Telas	
C030	xxxxxx	Laptop	Lenovo	Windows 10 Pro	Negocios Internacionales	XXXXXXXXXXXX
C029	xxxxxx	Laptop	Toshiba	Windows 8.1 Pro (2013)	Innovación y Desarrollo	XXXXXXXXXXXX
C028	xxxxxx	Desktop	INTEL	Windows 10 Pro	Innovación y Desarrollo	XXXXXXXXXXXX
C026	xxxxxx	Desktop	HP	Windows 10 Pro	Producción	XXXXXXXXXXXX
C024	xxxxxx	Desktop	HP	Windows 10 Pro	Mantenimiento Industrial	XXXXXXXXXXXX
C023	xxxxxx	Desktop	Altek	Windows 7 Professional	Guardianía	
C022	xxxxxx	Desktop	Quasad	Windows 10 Pro	Empaque	XXXXXXXXXXXX
	xxxxxx	Laptop	Dell	Windows 10 Home	Empaque	XXXXXXXXXXXX
C021	xxxxxx	Desktop	HP	Windows 7 Professional (2009)	Producción	XXXXXXXXXXXX
C019	xxxxxx	Desktop	HP	Windows 7 Professional (2009)	Producción (Bodega)	XXXXXXXXXXXX
C018	xxxxxx	Desktop	Intel	Windows 7 Professional (2009) Service Pack 1	Comedor	XXXXXXXXXXXX
C017	xxxxxx	Desktop	ATI	Windows 7 Professional (2009)	Producción	XXXXXXXXXXXX
C015	xxxxxx	Desktop	ALTEK	iMac	Marketing	
C014	xxxxxx	Desktop	HP	Windows 7 Professional (2009)	Carpintería	XXXXXXXXXXXX
C013	xxxxxx	Laptop	HP	Windows 10 Pro	Seguridad Ocupacional	
C013	xxxxxx	Laptop	Lenovo	Windows 10 Pro	Gerencia de Ventas	XXXXXXXXXXXX
C012	xxxxxx	Laptop	Dell	Windows 10 Pro	Producción	XXXXXXXXXXXX

ACTIVOS MATRIZ						
No. ARTÍCULO	**RESPONSABLE**	**TIPO**	**MARCA**	**DATOS PC**	**DEPARTAMENTO**	**NOMBRE DE EQUIPO**
C011	xxxxxx	Laptop	HP	Windows 10 Pro	Contabilidad	XXXXXXXXXXXX
C011	xxxxxx	Desktop	HP	Windows 7 Professional	Producción	XXXXXXXXXXXX
C011	xxxxxx	Laptop	Dell	Windows 10 Pro	Negocios Internacionales	XXXXXXXXXXXX
C010	xxxxxx	Laptop	Lenovo	Windows 10 Home	Presidencia Ejecutiva	XXXXXXXXXXXX
C009	xxxxxx	Laptop	HP	Windows 10 Pro	Negocios Internacionales	XXXXXXXXXXXX
C008	xxxxxx	Desktop	WINSTAR	Windows 10 Pro	Producción	XXXXXXXXXXXX
C007	xxxxxx		ASUS	Windows 10 Home	Producción	XXXXXXXXXXXX
C007	xxxxxx	Laptop	HP	Windows 7 Professional	Empaque	XXXXXXXXXXXX
C006	xxxxxx	Laptop	DELL	Windows 10 Pro	Tecnología	XXXXXXXXXXXX
C005	xxxxxx	Laptop	Dell	Windows 10 Pro	Innovación y Desarrollo	XXXXXXXXXXXX
	xxxxxx	Laptop	APPLE	MAC OS Big Sur (Versión 11.2.3)	Marketing	
	xxxxxx	Laptop	APPLE	MAC OS Sierra (Versión 10.12.6)	Marketing	
	xxxxxx	Desktop	Apple		Marketing	
	xxxxxx	Laptop	Lenovo	Windows 10 Pro	Gerencia de Finanzas	XXXXXXXXXXXX
	xxxxxx	Laptop	APPLE	macOS Mojave	Marketing	
	xxxxxx	Laptop	Dell	Windows 10 Home	Seguridad Ocupacional	XXXXXXXXXXXX
	xxxxxx	Laptop	Dell	Windows 10 Pro	Producción	
	xxxxxx	Desktop	Gigabyte Technology Co., Ltd.	Windows 7 Professional	Producción	XXXXXXXXXXXX
	xxxxxx	Laptop	Dell	Window 10	Proyectos	XXXXXXXXXXXX
	xxxxxx	Laptop	Dell	Window 10 Pro	Cobertura	XXXXXXXXXXXX
C0062	xxxxxx	Laptop	Dell	Windows 10 Pro	Negocios Internacionales	XXXXXXXXXXXX

ACTIVOS MATRIZ						
No. ARTÍCULO	**RESPONSABLE**	**TIPO**	**MARCA**	**DATOS PC**	**DEPARTAMENTO**	**NOMBRE DE EQUIPO**
C0063	xxxxxx	Laptop	Dell	Windows 10 Pro	Tecnología	XXXXXXXXXXXX
C0064	xxxxxx	Laptop	Dell	Windows 10 Pro	Tecnología	XXXXXXXXXXXX
IP008	xxxxxx	Ipad	Apple			
IP008	xxxxxx	Ipad	Apple			

Fuente: DPTO. SISTEMAS EMPRESA

**Los nombres de responsable y del equipo han sido ocultados por motivos de seguridad y confidencialidad.*

***Se ha eliminado información adicional de los equipos de la tabla por motivos de seguridad y confidencialidad.*

Como ya se mencionó, la empresa tiene políticas que rigen al respaldo de información, pero al no haber actualizado su matriz de activos este plan se lo puede considerar obsoleto, debido a que el software elegido para la automatización de respaldos ya no se encuentra instalado en los equipos de los empleados, por otro lado, la política de navegación en Internet, habla sobre las acciones que no se deben realizar considerando no consumir todo el ancho de banda de la red de la organización más no acciones que permitan precautelar la seguridad informática mediante el navegador web.

En la política de uso de equipos informáticos se establece en forma general que los dispositivos deben ser utilizados solamente para actividades laborales, adicional a esto, las cuentas de los usuarios sin permisos de administrador están imposibilitadas a instalar software, esto para evitar la instalación de malware, adicionalmente, la política ofrece las pautas para el proceso de asignación de equipos y detalla las responsabilidades de cada colaborador, tanto como del departamento de sistemas como del usuario.

Por otro lado, las normativas también sugieren que se establezca una matriz de riesgos, para poder medir la exposición de estos ante una posible amenaza, en la Tabla 11, se puede observar el escaso análisis de riesgos que presenta la organización para el procedimiento PR 122A, en las tablas 12, 13 y 14 se muestran las matrices de riesgos para las políticas PO 122B, PO 122C y PO 122D respectivamente.

Realizando un análisis a las matrices de riesgos mencionadas anteriormente se puede observar que la organización ha dado un primer paso a considerar políticas de ciberseguridad, sin embargo, estas se encuentran en un estado superficial, y poco o nada se han implementado controles de seguridad informática.

Tabla 11

Modelo de gestión del riesgo para las operaciones según la norma internacional BASC – PR 122A

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIONALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	**RIESGO**	**CONTEXTO**		**PARTES INTERESADAS**	**PROBABILIDAD**	**IMPACTO**	**EXPOSICIÓN**	**CLASIFICACIÓN DEL RIESGO**		**PLAN DE CONTINGENCIAS**	**SIMULACRO**	**CONSTANTES**	**PERIODICAS**	**ESPECÍFICAS**
Respaldo y Recuperación de Información	Pérdida total o parcial de información	**Fortaleza**	Asignación de perfiles de usuario al sistema central ERP Respaldos en la nube de BDD para poder acceder a los mismos desde cualquier lugar Acceso a videos de las diferentes exportaciones para validación de este Se cuenta con un plan de contingencia para poner operativo el sistema ERP	Interna: Todas las áreas de la compañía Externa: Desarrolladores externos con acuerdo de confidencialidad	0,6	0,8	0,48	ALTO	Capacitación de la políticas y procedimientos de la compañía Capsulas informativas de manejo de dispositivos, respaldos y seguridades	Difusión de la política de respaldos y recuperación de la información	Recuperación aleatoria de información	Seguimiento y verificación de respaldos de BDD e información de los usuarios críticos	Seguimiento y verificación de respaldos de BDD e información de los usuarios críticos Frecuencia: Trimestral	Cuando un usuario lo solicite o cuando se presente una incidencia
		Oportunidad	Se cuenta protocolo para respaldo de información de usuarios críticos Asignación de discos duros externos a						Mantener actualizado al Sophos	Revisión periódica de estatus del respaldo de BDD y de usuarios críticos				

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIONALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	**RIESGO**	**CONTEXTO**		**PARTES INTERESADAS**	**PROBABILIDAD**	**IMPACTO**	**EXPOSICIÓN**	**CLASIFICACIÓN DEL RIESGO**		**PLAN DE CONTINGENCIAS**	**SIMULACRO**	**CONSTANTES**	**PERIODICAS**	**ESPECÍFICAS**
			áreas críticas Poder acceder en tiempo real a las cámaras de seguridad de la empresa											
		Debilidad	Daño en discos duros externos otorgados a las áreas críticas En caso de pérdida de información solo se podrá recuperar hasta la última fecha y hora del respaldo programado Pedida de información de usuarios considerados no críticos						Revisión periódica de estatus de respaldos de información de usuarios					
		Amenaza	Circuito de cámaras de seguridad poseen puntos ciegos Perdida de información cuando se ha infiltrado						Revisión periódica de respaldos de BDD					

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIONALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	**RIESGO**	**CONTEXTO**		**PARTES INTERESADAS**	**PROBABILIDAD**	**IMPACTO**	**EXPOSICIÓN**	**CLASIFICACIÓN DEL RIESGO**		**PLAN DE CONTINGENCIAS**	**SIMULACRO**	**CONSTANTES**	**PERIODICAS**	**ESPECÍFICAS**
			algún rasomware y no se identificó de manera oportuna											

Fuente: DPTO. SISTEMAS EMPRESA

Tabla 12

Modelo de gestión del riesgo para las operaciones según la norma internacional BASC – PO 122B

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIONALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	**RIESGO**	**CONTEXTO**		**PARTES INTERESADAS**	**PROB.**	**IMPACTO**	**EXPOSICIÓN**	**CLASIFICACIÓN DEL RIESGO**		**PLAN DE CONTINGENCIAS**	**SIMULACRO**	**CONSTANTES**	**PERIODICAS**	**ESPECÍFICAS**
Contraseñas de Sistemas Informáticos	Accesos a información no autorizada	**Fortaleza**	Contar con una política para manejo se contraseñas de sistemas informáticos PO-122B El líder del procedo cuenta con usuarios maestros para acceder a los sistemas críticos	Interna: Todas las áreas de la compañía Externa: Desarrolladores externos con acuerdo de confidencialidad	0,6	0,4	0,24	ALTO	Capacitación de la políticas y procedimientos de la compañía	Difusión de la política de contraseñas	Simulacro de bloqueo de máquinas a una muestra de usuarios	Seguimiento y verificación de usuarios y administrador para acceso a los aplicativos Frecuencia: diario	Seguimiento y verificación de los procedimientos y políticas a través de los cambios masivos Frecuencia: semestral	Cuando un usuario lo solicite
		Oportunidad	Seguimiento a la ejecución de la política PO-122B						Verificar listados de usuarios activos en ERP	Manejo de archivo de credenciales maestras en caso empresa lo autorice				
		Debilidad	Los usuarios rehúsan contraseñas Los usuarios colocan contraseñas débiles Divulgar contraseñas entre usuarios						Desactivación o cambios de contraseña en correo institucional					

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIONALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	RIESGO	CONTEXTO		PARTES INTERESADAS	PROB.	IMPACTO	EXPOSICIÓN	CLASIFICACIÓN DEL RIESGO		PLAN DE CONTINGENCIAS	SIMULACRO	CONSTANTES	PERIODICAS	ESPECÍFICAS
		Amenaza	Accesos a información no autorizada Transaccionar con perfiles no autorizados Ingreso de malware para robo de información						Desbloqueo de usuarios por olvido de contraseñas					

Fuente: DPTO. SISTEMAS EMPRESA

Tabla 13

Modelo de gestión del riesgo para las operaciones según la norma internacional BASC – PO 122C

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIO-NALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	**RIESGO**	**CONTEXTO**		**PARTES INTERESADAS**	**PROBABILIDAD**	**IMPACTO**	**EXPOSICIÓN**	**CLASIFICACIÓN DEL RIESGO**		**PLAN DE CONTINGENCIA**	**SIMULACRO**	**CONSTANTES**	**PERIÓDICAS**	**ESPECÍFICAS**
Navegar en Internet	Ingreso de malware con mayor facilidad y/o saturación del ancho de banda	**Fortaleza**	Asignación de permisos de navegación a los dispositivos internos y externos de la compañía Contar con un dispositivo que permite controlar navegación y amenazas	Interna: Todas las áreas de la compañía Externa: Desarrolladores externos con acuerdo de confidencialidad	0,6	0,4	0,24	ALTO	Capacitación de la políticas y procedimientos de la compañía	Difusión de la política de navegación	Simulacro de navegación a una muestra de usuarios	Seguimiento y verificación de usuarios y administrador para acceso a los aplicativos Frecuencia: diario	Seguimiento y verificación de los procedimientos y políticas a través de los cambios masivos Frecuencia: semestral	Cuando un usuario lo solicite
		Oportunidad	Seguimiento a la ejecución de la política PO-122C						Mantener actualizado al Sophos	Revisión periódica de estatus del dispositivo en relación con las amenazas				

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIO-NALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	RIESGO	CONTEXTO		PARTES INTERESADAS	PROBABILIDAD	IMPACTO	EXPOSICIÓN	CLASIFICACIÓN DEL RIESGO		PLAN DE CONTINGENCIA	SIMULACRO	CONSTANTES	PERIÓDICAS	ESPECÍFICAS
		Debilidad	Usuarios con mayores privilegios hagan mal uso de estos						Asignación de permisos al dispositivo por MAC ADDRESS					
		Amenaza	Paginas nuevas que el firewall aun no los detecta como amenaza						Revisión de Incidencias en el Sophos					

Fuente: DPTO. SISTEMAS EMPRESA

Tabla 14

Modelo de gestión del riesgo para las operaciones según la norma internacional BASC – PO 122D

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIONALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	**RIESGO**	**CONTEXTO**		**PARTES INTERESADAS**	**PROBABILIDAD**	**IMPACTO**	**EXPOSICIÓN**	**CLASIFICACIÓN DEL RIESGO**		**PLAN DE CONTINGENCIAS**	**SIMULACRO**	**CONSTANTES**	**PERIODICAS**	**ESPECÍFICAS**
Uso Equipos Informáticos	Disminución de la vida útil y del rendimiento del equipo	**Fortaleza**	Contar con una política para uso de equipos informáticos PO-122D El área de tecnología posee un listado de los equipos informáticos de la compañía	Interna: Todas las áreas de la compañía Externa: Desarrolladores externos con acuerdo de confidencialidad	0,6	0,4	0,24	ALTO	Capacitación de la políticas y procedimientos de la compañía	Difusión de la política de uso de equipos electrónicos				Cuando haya movimiento de equipos. Cuando el incidente se presente
		Oportunidad	Seguimiento a la ejecución de la política PO-122D						Mantener actualizado el listado de equipos activos en la compañía	Manejo del archivo actualizado de equipos de computación				

IDENTIFICAR EL RIESGO					ANALIZAR Y EVALUAR EL RIESGO				CONTROLES OPERACIONALES	RESPUESTA A EVENTOS		REVISIONES		
PROCESO	**RIESGO**	**CONTEXTO**		**PARTES INTERESADAS**	**PROBABILIDAD**	**IMPACTO**	**EXPOSICIÓN**	**CLASIFICACIÓN DEL RIESGO**		**PLAN DE CONTINGENCIAS**	**SIMULACRO**	**CONSTANTES**	**PERIODICAS**	**ESPECÍFICAS**
		Debilidad	Los usuarios no notifican de algún cambio Equipos que se cambian partes y piezas Negligencia en el manejo del equipo por parte del usuario						Control de instalación de programas no autorizados					
		Amenaza	Robos, daño de equipos.											

Fuente: DPTO. SISTEMAS EMPRESA

La situación descrita anteriormente se debe a que el departamento de sistemas no cuenta con el personal necesario como para evaluar y gestionar la ciberseguridad dentro de la organización, y han hecho lo mínimamente necesario para mantener los sistemas en funcionamiento y quizá han contado con la suerte de no ser víctima de algún ataque informático.

Con toda la información expuesta hasta el momento se puede concluir que la organización no es ajena a la gestión de ciberseguridad, ya sea de manera consciente o por la obligación de considerarla desde las exigencias de BASC, sin embargo, estas medidas no siguen una hoja de ruta, no existe un panorama claro de los hitos a alcanzar en materia de ciberseguridad a través del tiempo, tampoco cuentan con un proceso claro de evaluación y gestión de riesgos y amenazas, y en algo cuentan con medidas de continuidad del negocio. Además, tampoco existe un programa de capacitación al personal en temas de ciberseguridad, fuera de pequeños “tips” de información sobre ciberseguridad comunicados mediante correo electrónico, es necesario que la organización comience a implementar controles de seguridad informática para que en un futuro pueda gestionar de manera adecuada su seguridad informática.

CAPÍTULO IV

MARCO DE REFERENCIA PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA DE FABRICACIÓN, COMERCIALIZACIÓN Y EXPORTACIÓN DE MUEBLES

4.1. Introducción

Al hablar de ciberseguridad dentro de las organizaciones, se abre un amplio escenario de acción, desde capacitar y entrenar a las personas para prevenir ataques cibernéticos hasta implementar soluciones tecnológicas que protejan la infraestructura informática de las empresas, como ya se había mencionado en este documento, implementar controles de seguridad informática es una tarea titánica, tanto para los profesionales como para las organizaciones. Bien se pueden tomar un sin número de medidas de ciberseguridad dentro de una empresa para proteger la infraestructura tecnológica y la información, sin embargo, siempre se debe considerar el impacto que estas tendrán sobre los procesos del giro de negocio y el personal que los lleva a cabo, la implementación de los controles debe buscar el equilibrio entre las normas de seguridad y el correcto desenvolvimiento de las actividades laborales de la organización.

Cobb (2019) en su artículo "Guía de Ciberseguridad para Pequeñas Empresas" propone los siguientes pasos para comenzar a implementar controles de seguridad dentro de una empresa:

- Analizar los activos con los que cuenta la organización.

- Identificar riesgos y amenazas de los activos.
- Crear políticas que permitan gestionar la seguridad de la información e infraestructura tecnológica.
- Elegir e implementar los controles que permitan aplicar las políticas creadas.
- Capacitar y concientizar al personal sobre seguridad.

Las normativas NIST y CIS detallan en sus primeros controles el levantamiento de activos, por el contrario, la norma ISO 27001 comienza por determinar las políticas de ciberseguridad y en los siguientes puntos se centra en implementar controles, esto último puede ser confuso para una empresa que apenas ha comenzado a tratar su ciberseguridad, debido a que puede ser difícil establecer políticas sin tener claro el contexto actual de la ciberseguridad en la organización, dicho contexto será propio de cada empresa.

Por lo anterior se considera que la normativa adecuada, que servirá de base para el desarrollo de un marco de referencia para la empresa de fabricación, comercialización y exportación de muebles es la normativa CIS en su versión 8, porque ha simplificado la aplicación de controles dentro de compañías pequeñas o que apenas comienzan a tomar medidas de ciberseguridad y según lo analizado en el capítulo anterior, la empresa que es objeto de estudio del presente trabajo de tesis ha tomado ciertas medidas de ciberseguridad, sin embargo, estas carecen de un guía central que permita tomar medidas de seguridad informática de mejor manera, adicionalmente se tomarán algunos aspectos relevantes del estándar NIST para la creación de este marco de referencia, como la guía para un programa de entrenamiento NIST 800-50.

4.2. Desarrollo del Marco de Referencia

El marco de referencia propuesto para la empresa de fabricación, comercialización y exportación de muebles consistirá en un proceso cíclico que cuenta con etapas para identificar, planificar, proteger y capacitar, como se muestra en la siguiente figura:

Figura 4 - Fases de Marco de Referencia
Fuente: Autor

Se ha determinado estas cuatro etapas debido a que son aplicables a todos los controles de seguridad del IG1 de la normativa CIS versión 8, en cada control se debe identificar los activos sobre los que se debe trabajar o el estado en el que se encuentra la empresa con relación a dicho control.

Nada se puede ejecutar sin una previa planificación que permita medir de alguna manera los esfuerzos a invertir en la implementación de cada control de seguridad, esta planificación se basará en un análisis de riesgos de esta forma se podrá determinar la prioridad de las acciones a tomar.

El fin mismo de un marco de referencia es el de otorgar una guía a seguir para la protección de activos y/o información, en la tercera etapa del marco de referencia se

aborda las consideraciones a tomar en cuenta al momento de aplicar la medidas de seguridad y por último, una vez protegidas la vulnerabilidades encontradas en la organización, es necesario que el personal directamente involucrado en las medidas de seguridad sean debidamente capacitadas, para que dichas medidas se mantenga en el tiempo y puedan ser sometidas a un proceso de mejora continua.

En este marco de referencia se busca establecer medidas simples y sencillas para que la empresa de fabricación, comercialización y exportación de muebles pueda implementar controles de seguridad y se encuentre protegida ante cualquier ataque informático que se pueda dar en un escenario cotidiano o en un nuevo confinamiento.

4.2.1. Identificar

En la primera etapa del marco de referencia, se busca identificar la situación actual de la empresa con relación al control de seguridad tratado en ese momento, a esto se lo denominará contexto, habrá controles en los cuales la organización tenga un avance en la implementación, esto permitirá centrar los esfuerzos en crear o mejorar los procesos de control. En esta fase se debe recopilar toda la información posible con la que cuente la empresa con relación al control de seguridad tratado en ese momento.

Para comenzar a levantar el contexto se debe evaluar todas las implicaciones que el control trae consigo, tales como:

- **Objetivo(s) del control –** Es importante aclarar la finalidad del control de seguridad para establecer de manera clara y concisa el alcance de este y de esta forma poder tener una forma de evaluar si se ha podido aplicar el control total o parcialmente.
- **Valor agregado que puede otorgar el control a la organización –** Para validar ante el nivel gerencial la importancia de implementar un control de seguridad dentro de la organización, es importante evidenciar cuál es el valor

agregado que este puede otorgar a la empresa, esto con el fin de obtener el apoyo y compromiso de las autoridades al momento de aplicar el control de seguridad, dicho apoyo se puede ver reflejado en: la asignación de recursos económicos o humanos, delegación de responsabilidades, toma de decisiones, y/o dictado de políticas.

- **Antecedentes de implementación –** Por uno u otro motivo la organización pudo haber implementado el control de seguridad tratado en ese momento, en este caso, es importante determinar si la aplicación de dicho control se mantiene activa y se lo está monitoreando o determinar la razones por las que no se ha dado el seguimiento correspondiente, dichas razones pueden ser por ejemplo: falta de personal calificado, no asignación de recursos económico o inexistencia de políticas que apoyen a la aplicación del control de seguridad. Este es el punto que establece el contexto histórico de la empresa con relación al control de seguridad tratado, es aquí donde se puede evidenciar en una primera instancia los posibles esfuerzos que se deben realizar al implementar el control de seguridad, con esto se puede optimizar dichos esfuerzos al no volver a ejecutar trabajo ya realizado.
- **Políticas que regulen la implementación del control –** De haberse implementado con anterioridad dentro de la organización el control de seguridad tratado, dicho control podría estar respaldado con una política organizacional, de ser este el caso, se debe evaluar si esta política se cumple; en el escenario de no darse cumplimiento, es necesario determinar las razones para poder tomar medidas con el fin de establecer esta política dentro de la cultura organizacional, puesto que todos el personal debe ser consiente del papel que tiene dentro de la ciberseguridad de la empresa. Por otro lado, de no

existir política alguna con relación al control de seguridad tratado, esta debe ser redactada, de esta forma los esfuerzos realizados al implementar el control de seguridad no serán en vano y se mantendrán en el tiempo con el respaldo de dicha política. Cabe aclarar que el cumplimiento de las políticas organizacionales moldea en el mediano y largo plazo la cultura organizacional y dentro de esta debe ser considerado el tratamiento de la ciberseguridad.

Todo lo mencionado anteriormente puede estar respaldado con uno o varios documentos, sin embargo, como propuesta dentro de este marco de referencia a continuación se muestra un formato de resumen del contexto del punto de control a evaluar, este formato busca ser una herramienta para presentar de forma tabulada toda la información recopilada en la fase de identificación y de esta manera facilitar su análisis.

Tabla 15
Formato de resumen de análisis de contexto

FORMATO DE ANÁLISIS DE CONTEXTO DE PUNTOS DE CONTROL CIS				
Punto de control				
Número	Número del control de seguridad dentro de la Normativa CIS.			
Título	Nombre del control de seguridad a tratar.			
Objetivo	Alcance que pretende el control de seguridad.			
Valor agregado	Valor agregado que otorga el control de seguridad a la organización.			
Resumen de Antecedes				
Implementado	Si	Marcar una x si se ha implementado	No	Marcar una x si no se ha implementado
Porcentaje de implementación		% Porcentaje considerado de implementación en caso de si haber sido implementado.		
Políticas de uso	Si	Marcar una x si existe política	No	Marcar una x si no existe política
Documento de la política	Nombre de el o los documentos que detallan la política			
Observaciones de Antecedentes				
Listado de las observaciones a destacar con relación al control de seguridad tratado dentro de la organización.				

En el Anexo B se facilita el formato de resumen del contexto del punto de control a evaluar en blanco.

4.2.2. Planificar

La segunda fase del marco de referencia tiene como objetivo planificar la manera en la que el control tratado en ese momento se aplicará, para definir este proceso la herramienta a utilizar será el análisis de riesgos, como ya se ha mencionado en el Capítulo II de este trabajo, un riesgo es la probabilidad que una vulnerabilidad sea explotada multiplicada por el impacto que dicha explotación tenga en la organización. Los riesgos deben ser analizados de acuerdo con la realidad de la empresa, un riesgo de alto impacto en la organización A puede considerarse de menor impacto en una organización B.

La gestión de riesgos por sí misma es un tema extenso que sobrepasa el alcance de este trabajo, sin embargo, a continuación, se plantean pasos básicos a seguir para realizar el análisis de riesgos en la empresa.

- **Determinar vulnerabilidades –** Reconocer las debilidades que pueden ser explotadas con relación al punto de control a tratar en ese momento.
- **Determinar fuentes de amenazas –** Establecer las acciones que podría explotar una vulnerabilidad lo que ocasionaría que los procesos productivos de la empresa se vean afectados en mayor o menor medida.
- **Determinar la probabilidad de ocurrencia –** En este punto se debe evaluar la probabilidad que una vulnerabilidad sea explotada en la organización, para determinar esta probabilidad se puede apoyar en datos de la frecuencia con la que cierta amenaza a ocurrido en el pasado, por ejemplo: suponiendo que en el último mes en la empresa, 4 de cada 10 computadores han sido infectados por algún tipo de malware, esto daría un 0.4 de probabilidad que un equipo sea contaminado en un futuro. Para facilitar el cálculo del riesgo se recomienda asignar pesos definidos a la probabilidad de ocurrencia de una amenaza, basada en la siguiente escala: Improbable=0, Poco probable=0.25,

Probable=0.5, Muy probable=0.75, Seguro=1; basados en el ejemplo anterior 0.4 se acerca al peso de 0.5 en la escala de probabilidad, por lo que la amenaza es “Probable” que suceda.

No es de extrañar que la organización, por apenas encontrarse en la fase inicial de implementación de controles de ciberseguridad, no cuente con la información histórica de la frecuencia de ocurrencia de alguna amenaza, por lo que se podría considerar que la mayoría de estas serían catalogadas como improbables, esto provocaría que los riesgos lleguen a considerarse nulos, para evitar estos casos la escala de probabilidad a utilizar será la siguiente:

- **Poco probable: 0.25**
- **Probable: 0.50**
- **Muy probable: 0.75**

El peso de “Seguro=1” de igual forma ha sido omitido de la escala, debido a que también sería fácil encasillar en esta categoría a todas las amenazas, se puede cometer el error de asegurar que pueden ocurrir debido a la falta de controles de ciberseguridad en la empresa.

- **Determinar la magnitud de impacto –** La magnitud del impacto hace referencia a cuan grave sería para la organización que alguna amenaza llegue a ocurrir, en este paso pueden existir varios criterios para determinar el impacto de la amenaza, tales como: las pérdidas económicas, el costo de recuperación, afectación al rendimiento del trabajo, daños a la imagen de la empresa, entre otros. Una forma de determinar la magnitud del impacto de la ocurrencia de una amenaza puede basarse en el análisis de los escenarios que deriven de un ataque, por ejemplo: ¿cuántas ventas dejaría de hacer un asesor comercial en el caso que sea imposible acceder a la información almacenada

en su computador?, ¿cuán complejo sería recuperar o volver a generar toda la información?, ¿es de alto impacto para el usuario y para la organización? Según el análisis de estos criterios, se pude valorar la magnitud del impacto basados en la siguiente escala:

- **Bajo: 0.25**
- **Medio: 0.50**
- **Alto: 0.75**

Otro factor que ayudaría a determinar la magnitud del impacto es el de determinar si dicha amenaza atenta directamente contra la confidencialidad, integridad y/o disponibilidad de la información, el impacto podría ser mayor si la amenaza afecta a las tres dimensiones de la seguridad que a una en especial.

- **Determinar el riesgo –** Una vez determinada la probabilidad de ocurrencia de una amenaza y la magnitud del impacto que esta tendría dentro de la organización, se puede calcular el riesgo de cada una de las amenazas, que según lo establecido en este marco de referencia se resume en la siguiente tabla:

Tabla 16
Tabla de cálculo de riesgo

		PROBABILIDAD		
		0.25	0.50	0.75
IMPACTO	0.25	**0.06**	**0.13**	**0.19**
	0.50	**0.13**	**0.25**	**0.38**
	0.75	**0.19**	**0.38**	**0.56**

Fuente: Autor

De esta forma se clasifica el riesgo de la siguiente manera:

- Riesgo de nivel bajo, menor o igual a 0.13
- Riesgo de nivel medio, entre 0.13 y 0.25
- Riesgo de nivel alto, mayor a 0.25

En el Anexo C se muestra un formato de matriz de análisis de riesgos que pretende ayudar en la tarea del análisis de riegos.

Una vez detallado el análisis de riesgos referente al control de seguridad tratado en ese momento, la prioridad con los que se tratará cada uno de ellos será la siguiente: los riesgos catalogados de nivel “alto” deben ser los primeros en gestionarse ya sea mitigándolos o transfiriendo su tratamiento a un tercero, de la misma forma se procederá con los riesgos de nivel “medio” y por último los de nivel “bajo”.

En esta misma etapa se puede determinar el plan de tratamiento de los riesgos, este plan consistirá en las actividades a realizar para mitigar, transferir o aceptar el riesgo.

4.2.3. Proteger

Una vez revisado el contexto junto con la planificación realizada mediante el análisis de riesgos, se procederá a implementar las medidas a tomar para el control de seguridad tratado en el momento. Las medidas a aplicar pueden ser de dos tipos: creación o modificación de procesos para precautelar la seguridad y/o la implementación de herramientas informáticas de ciberseguridad. Estas medidas deben ser aplicadas según el contexto de la empresa, acorde a la capacidad de los recursos que esta pueda asignar tanto económicos como humanos.

- **Creación o modificación de procesos de la empresa –** En determinadas ocasiones, luego del análisis de riesgo se puede determinar la creación o modificación de algún proceso dentro del flujo del giro de negocio que sirva para precautelar la seguridad de los activos y/o la información, este marco de referencia recomienda tomar en cuenta las siguientes consideraciones:
    - El proceso debe ser lo más simple y sencillo de ejecutar.
    - No debe ser un obstáculo para el correcto desenvolvimiento de las actividades diarias del personal.

- En el mejor de los casos debe buscar dar un valor agregado a la organización.

- **Implementación de herramientas informáticas de ciberseguridad –** Si se decide que la implementación de una herramienta informática es lo necesario para el control a tratar, la adquisición de esta debe estar acorde a la realidad económica y capacidad técnica de la empresa. Como puntos a tomar en cuenta para la selección de una herramienta informática se recomienda:
  - Analizar dos o más alternativas de la herramienta en el mercado (libres y de paga).
  - Comparar las herramientas seleccionadas en cuanto a características, relación costo-beneficio, opiniones de usuarios en sitios web o blog especializados.
  - De ser posible realizar una prueba de concepto con las herramientas consideradas más idóneas para la empresa.

Posterior a esto la empresa a través de sus gerencias deberá establecer las políticas organizacionales que acompañarán al cumplimiento de las medidas de ciberseguridad tomadas. En estas políticas se determinarán roles, responsables y procedimientos para cada uno de los casos establecidos en los controles de seguridad; el fin de proponer la generación de políticas en este punto, es comenzar a establecer dentro de la organización la cultura de gestión de ciberseguridad, para que en un futuro no sea nuevo la creación de dichas políticas en el caso que se desee implementar otro marco de referencia.

4.2.4. Capacitar

Esta fase de este marco de referencia considera a la capacitación como la preparación o desarrollo de habilidades a los roles establecidos en cada uno de los controles, esto con el fin de crear conciencia sobre la importancia de la ciberseguridad dentro de la empresa

y también desarrollar capacidades en el personal de la empresa que permita tener actores proactivos e involucrados en las medidas de seguridad implementadas.

Las actividades de capacitación a ejecutar deben estar acorde a las medidas de seguridad tomadas en la fase anterior, por ejemplo, si se decidió modificar un proceso para garantizar la seguridad de algún tipo de información, se deberá capacitar al personal directamente relacionado con dicho proceso para garantizar su cumplimiento, por otro lado, si la medida fue implementar una herramienta informática, la capacitación será dirigido al personal que gestionará dicha herramienta.

Basados en la publicación especial NIST 800-50 para este marco de referencia se recomienda los tres componentes necesarios en programa de capacitación:

- **Concienciación** – Los usuarios deben comprender la importancia de las medidas de seguridad.
- **Entrenamiento –** Los usuarios deben desarrollar habilidades referentes a las medidas de seguridad tomadas en la organización.
- **Educación -** La educación integra todas las habilidades de seguridad desarrolladas y buscar formar profesionales con visión y respuesta proactiva.

La capacitación debe buscar crear conciencia en el usuario para que este asimile la importancia de la medida de seguridad y de este modo el entrenamiento en cuanto a la ejecución de los procesos y/o del manejo de la herramienta informática de ciberseguridad tendrá mejor efecto, la finalidad de esta capacitación es tener profesionales formados en medidas de seguridad.

4.3. Fases de implementación de puntos de control de seguridad informática dentro del marco de referencia

Implementar todos controles de seguridad informática, es un proyecto a largo plazo, en el cual intervienen factores como la disponibilidad de los recursos económicos y los

recursos de capital humano, además con base en el análisis situacional de la organización, se puede asegurar que no se dispone del personal suficiente para implementar todos los puntos de control del IG1 de manera rápida y eficiente, por lo que, considerando las capacidades organizacionales, se plantea seguir la aplicación de los controles del IG1 en el orden sugerido por la normativa CIS.

Dentro de IG1 existen 15 controles establecidos por la normativa CIS, como se mencionó al inicio de este capítulo, las etapas de este marco de referencia se deben aplicar de forma cíclica, es decir, se ejecutará 14 veces el proceso de identificar, planificar, proteger y capacitar, una vez por cada control a aplicar, en la Tabla 17 se especifica las 14 fases determinados para la implementación de los controles de seguridad.

Cabe aclarar que implementar todos los controles del grupo de implementación uno (IG1) de la normativa CIS versión 8 sobrepasa los límites de este trabajo de tesis, debido a que aplicar el marco de referencia a cada uno de los quince controles es un trabajo a realizarse en el largo plazo en la empresa de fabricación, comercialización y exportación de muebles, sin embargo, a continuación se procederá a implementar los dos primeros controles de IG, inventario y control de activos de hardware y software, para demostrar la aplicación del marco de referencia, se considera que no hay inconvenientes para ejecutar estos dos controles paralelamente.

Tabla 17
Fases de Marco de Referencia

Fase	Etapas	Control CIS	Título	Descripción
Fase 1	Identificar Planificar Proteger Capacitar	**1**	Inventario y control de activos empresariales	Inventariar, rastrear y corregir todos los activos tecnológicos de la empresa conectados a la infraestructura física, virtual, remota y aquellos dentro de entornos de nube, para conocer con precisión la totalidad de los activos que deben monitorearse y protegerse dentro de la empresa. Esto también apoyará la identificación de activos no autorizados para eliminar o remediar.
	Identificar Planificar Proteger Capacitar	**2**	Inventario y control de activos de software	Inventariar, rastrear y corregir todo el software (sistemas operativos y aplicaciones) en la red para que solo se instale y pueda ejecutarse el software autorizado, y que se impida la instalación o ejecución de software no autorizado.
Fase 2	Identificar Planificar Proteger Capacitar	**3**	Protección de datos	Desarrollar procesos y controles para identificar, clasificar, manejar, retener y eliminar datos de forma segura.
Fase 3	Identificar Planificar Proteger Capacitar	**4**	Configuración segura de activos y software	Garantizar la configuración segura de los activos empresariales de hardware y software.

Fase	Etapas	Control CIS	Título	Descripción
Fase 4	Identificar Planificar Proteger Capacitar	**5**	Gestión de cuentas	Utilizar procesos y herramientas para asignar y administrar la autorización de credenciales para cuentas de usuario, incluidas cuentas de administrador, así como cuentas de servicio, para activos y software empresariales.
Fase 5	Identificar Planificar Proteger Capacitar	**6**	Gestión del control de acceso	Usar procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos de hardware y software empresariales.
Fase 6	Identificar Planificar Proteger Capacitar	**7**	Gestión continua de vulnerabilidades	Desarrollar un plan monitorear continuamente las vulnerabilidades en todos los activos dentro de la infraestructura organizacional, con el fin de remediar y minimizar la ventana de oportunidad para los atacantes.
Fase 7	Identificar Planificar Proteger Capacitar	**8**	Gestión de registros de auditoría	Recopilar, alertar, revisar y conservar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

Fase	Etapas	Control CIS	Título	Descripción
Fase 8	Identificar Planificar Proteger Capacitar	**9**	Protecciones de correo electrónico y navegador web	Mejorar las defensas y detecciones de amenazas del correo electrónico y los vectores web, ya que estas son oportunidades para que los ciberdelincuentes manipulen el comportamiento humano a través de la participación directa.
Fase 9	Identificar Planificar Proteger Capacitar	**10**	Defensas contra malware	Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, código o scripts malintencionados en activos empresariales.
Fase 10	Identificar Planificar Proteger Capacitar	**11**	Recuperación de datos	Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales dentro del ámbito a un estado previo al incidente y de confianza.
Fase 11	Identificar Planificar Proteger Capacitar	**12**	Gestión de la infraestructura de red	Establecer, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, para evitar que los atacantes exploten los servicios de red y puntos de acceso vulnerables.

Fase	Etapas	Control CIS	Título	Descripción
Fase 12	Identificar Planificar Proteger Capacitar	**15**	Gestión de proveedores de servicios	Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales, o son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.
Fase 13	Identificar Planificar Proteger Capacitar	**17**	Gestión de respuesta a incidentes	Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes para preparar, detectar y responder rápidamente a un ataque.

Fuente: Autor

Hasta este punto, se ha determinado las necesidades de la organización con relación a la ciberseguridad, se ha establecido la ruta a seguir para implementar los controles determinados en el IG1 (grupo de implementación 1), de la normativa CIS versión 8, adicional se mostró el valor agregado que cada punto de control otorga a la empresa alineando a los intereses de la organización, y se determinó el ciclo de trabajo a seguir para implementar cada punto, que consta de los siguientes fases: identificar, planificar, proteger y capacitar.

En el desarrollo del marco de referencia en este trabajo de tesis no se consideró una etapa de monitoreo y/o control, debido a que estas actividades se encuentran detalladas en los grupos de implementación 2 y 3 de la normativa CIS versión 8, es decir, dicha etapa se la considerará una vez implementados los controles del IG1. Las actividades para desarrollar dentro de la etapa de monitoreo y/o control, consistirán en establecer mecanismo de revisión continua del estado de los activos y sus vulnerabilidades generalmente apoyados por herramientas informáticas dedicadas para este fin.

4.4. Aplicación del marco de referencia con la implementación de controles de gestión de activos de hardware y software

Para generar una mejor visualización de la aplicación del marco de referencia desarrollado en este trabajo de tesis, se ha aplicará este dentro de la empresa de fabricación, comercialización y exportación de muebles a partir de su situación actual en temas de ciberseguridad.

Según lo detallado en el análisis situacional del presente trabajo, la empresa de fabricación, comercialización y exportación de muebles posee medidas de seguridad ya implementadas, tales como: tener un listado del inventario de hardware de la compañía en formato de hoja de cálculo, la creación dentro de los computadores del personal de dos cuentas, la primera con privilegios de administrador y una o más con permisos limitados

de usuario, dentro de la red informática de la empresa existe un firewall que filtra las conexiones de todos los equipos conectados a la red; adicional a esto cuentan con cinco políticas que promueven el manejo del espacio del trabajo, gestión de las conexiones web, uso de equipos y gestión de contraseñas.

Con breve análisis se puede establecer en menor o mayor medida la situación actual de la empresa donde se desea aplicar el marco de referencia, sin embargo, en este marco se han definido etapas a seguir para la implementación de cada control, y se ha definido seguir el orden establecido en los controles del IG1 de CIS versión 8, es decir, los primeros controles a aplicar son los de gestión de activos de hardware y software.

4.4.1. Etapa Identificar

En CIS versión 8, los controles uno y dos detallan la gestión de activos de hardware y software (Tabla 18), estos se centran en identificar dichos activos y responder ante los que no se encuentra autorizados, en este caso se seleccionará implementar los dos controles debido a que se considera que se puede levantar el inventario de hardware y software de forma paralela.

Tabla 18
Controles de gestión de activos de hardware y software CIS versión 8

1	**Inventario y control de activos de hardware empresariales**		
Control CIS	**Salvaguardia CIS**	**Acción de seguridad**	**Título**
1	1,1	Identificar	Crear y gestionar un inventario detallado de activos empresariales
1	1,2	Responder	Abordar activos no autorizados
2	**Inventario y control de activos de software**		
Control CIS	**Salvaguardia CIS**	**Acción de seguridad**	**Título**

2	2,1	**Identificar**	Crear y gestionar un inventario de software
2	2,2	**Identificar**	Garantizar que el software autorizado sea compatible actualmente
2	2,3	**Responder**	Abordar software no autorizado

Fuente: Normativa CIS versión 8

- **Punto de control 1 – Inventario y control de activos de Hardware**

Este punto de control busca manejar activamente todos los dispositivos de hardware dentro de la organización, para conocer todos los activos que deben monitorearse y protegerse (CIS, 2021). Este punto de control se alinea a los intereses organizacionales de la siguiente manera:

  - Permite manejar presupuestos de mantenimiento, renovación y adquisición de equipos.
  - Se puede elaborar un plan de mantenimiento de dispositivos para prevenir fallos que afecten al desarrollo de la actividad laboral.
  - Con el monitorio activo de los dispositivos se puede prevenir el uso incorrecto de los equipos, que puedan afectar a la información que estos contienen o a su vida útil.

- **Punto de control 2 – Inventario y control de activos de Software**

Control que tiene como objetivo gestionar todo el software en la red, y que se impida la instalación o ejecución de software no autorizado dentro de la organización (CIS, 2021). Este punto de control se alinea a los intereses organizacionales de la siguiente manera:

  - Permite manejar presupuestos para adquisición y renovación de licencias.

- Busca el uso de software seguro, descargado de fuentes oficiales y conocidas.
- Monitorea la ejecución de software malicioso ejecutado en los equipos de la red.

4.4.1.1. Análisis de contexto

Dentro del análisis de contexto realizado a la organización, se encontró un indicio de manejo de inventario de activos de hardware, sin embargo, no existe una política detallada que lo respalde.

En el siguiente cuadro se muestra un resumen del análisis del contexto de este punto de control.

Tabla 19
Resumen de análisis de contexto de punto de control 1 de CIS

FORMATO DE ANÁLISIS DE CONTEXTO DE PUNTOS DE CONTROL CIS				
Punto de control				
Número	1			
Título	INVENTARIO Y CONTROL DE ACTIVOS DE HARDWARE			
Objetivo	Manejar activamente todos los dispositivos de hardware dentro de la organización, para conocer todos los activos que deben monitorearse y protegerse			
Valor agregado	- Permite manejar presupuestos de mantenimiento, renovación y adquisición de equipos. - Se puede elaborar un plan de mantenimiento de dispositivos para prevenir fallos que afecten al desarrollo de la actividad laboral. - Con el monitorio activo de los dispositivos se puede prevenir el uso incorrecto de los equipos, que puedan afectar a la información que estos contienen o a su vida útil.			
Resumen de Antecedes				
Implementado	Si	X	No	
Porcentaje de implementación	10	%		
Políticas de uso	Si		No	X
Documento de la política				
Observaciones de Antecedentes				
• La organización cuenta con una matriz de inventario de activos de hardware, sin embargo, esta se encuentra desactualizada.				

- Este inventario es llevado en una hoja de cálculo.
- Por la cantidad de dispositivos, llevar el inventario en una hoja de cálculo es inviable.
- No existe un método de monitorea de activos de hardware.
- No existe un proceso centralizado de control de acceso a los activos.

Fuente: Autor

Tabla 20
Resumen de análisis de contexto de punto de control 2 de CIS

FORMATO DE ANÁLISIS DE CONTEXTO DE PUNTOS DE CONTROL CIS				
Punto de control				
Número	2			
Título	INVENTARIO Y CONTROL DE ACTIVOS DE SOFTWARE			
Objetivo	Gestionar todo el software en la red, y que se impida la instalación o ejecución de software no autorizado dentro de la organización.			
Valor agregado	- Permite manejar presupuestos para adquisición y renovación de licencias. - Busca el uso de software seguro, descargado de fuentes oficiales y conocidas. - Monitorea la ejecución de software malicioso ejecutado en los equipos de la red.			
Resumen de Antecedes				
Implementado	Si		No	X
Porcentaje de implementación	0	%		
Políticas de uso	Si		No	X
Documento de la política				
Observaciones de Antecedentes				
• La organización no cuenta con una matriz de inventario de activos de software. • Por la cantidad de dispositivos, llevar el inventario en una hoja de cálculo es inviable. • No existe un método de monitoreo de activos de software.				

Fuente: Autor

Una vez construidas las tablas de resumen del contexto se puede concluir que a pesar de contar con un gran número de activos de hardware y software estos no se encuentran inventariados y peor aún se los monitorea, esto implica que el análisis de riesgos se lo debe aplicar desde cero.

4.4.2. Etapa Planificar

En esta etapa levantara mediante el análisis de riesgos las vulnerabilidades que puede aquejar a la organización al no contar con un inventario de activos de hardware y software, en este caso el objeto a proteger es la organización debido a que a través de sus activos puede estar expuesta a diferentes tipos de amenazas.

Como primer paso dentro de esta etapa se estableció que se debe determinar las vulnerabilidades existentes con relación al control tratado, en este caso, inventario y control de activos de hardware y software.

- **Determinar vulnerabilidades de inventario de activos de hardware**
    - No poder evaluar y cuantificar el alcance de los daños ocasionados por la materialización de alguna amenaza física sobre los dispositivos por no contar con un registro actualizado de activos de hardware.
    - Dificultad para ejecutar otros controles de seguridad por no poder medir el esfuerzo necesario que se debe realizar para proteger los activos de hardware.

Una vez establecidas las vulnerabilidades se procederá a realizar el análisis de riesgos desde la matriz detallada en el Anexo C.

Tabla 21

Matriz de riesgos de control – Inventario y control de activos de hardware

MATRIZ DE ANÁLISIS DEL RIESGO																
Vulnerabilidad	**AMENAZA**	**Tipo**		**¿Qué afecta?**			**CONSECUENCIAS**	**Probabilidad**			**Impacto**			**Resultado**	**Riesgo**
		Interna	**Externa**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**0.25**	**0.50**	**0.75**	**0.25**	**0.50**	**0.75**		
No poder evaluar y cuantificar el alcance de los daños ocasionados por la materialización de alguna amenaza física sobre los dispositivos por no contar con un registro actualizado de activos de hardware.	Robo o pérdida de equipos		X	X		X	Pérdida de información. Imposibilidad de realizar actividades laborales del usuario.	X				X		0.13	BAJO
	Fin de vida útil del equipo	X				X	Costos inesperados de reposición que afectan al presupuesto. Daño inesperado del equipo lo que imposibilitaría acceder a la información.	X				X		0.13	BAJO
	Equipos usados sin autorización dentro de la organización.		X	X	X	X	Interrupción del normal desempeño de otros dispositivos. Posibles fuentes de fugas de información.		X			X		0.25	MEDIO

MATRIZ DE ANÁLISIS DEL RIESGO																
Vulnerabilidad	**AMENAZA**	**Tipo**		**¿Qué afecta?**			**CONSECUENCIAS**	**Probabilidad**			**Impacto**			**Resultado**	**Riesgo**
		Interna	**Externa**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**0.25**	**0.50**	**0.75**	**0.25**	**0.50**	**0.75**		
Dificultad para ejecutar otros controles de seguridad por no poder medir el esfuerzo necesario que se debe realizar para proteger los activos de hardware.	Equipos desconocidos conectados a la red informática.	X		X	X	X	Imposibilidad de integrar al dispositivo al plan de ciberseguridad.			X	X			0.19	MEDIO
	Imposibilidad de evaluar configuraciones de los equipos.	X		X	X	X	Filtración de información confidencial. Consumo adicional de recursos del equipo o de la red. Contaminación de equipos de la red con malware.			X		X		0.19	MEDIO

Fuente: Maestría de Ciberseguridad UISEK
Elaborado por: Autor

Una vez realizado el análisis de riesgos se puede determinar que existe en promedio un riesgo “medio” en la organización al no contar con un inventario de activos de hardware, pues bien, las amenazas detallas pueden afectar a un número reducido de usuarios, lo que no afectaría en gran medida los procesos productivos de la organización.

El plan de tratamiento del riesgo sería el siguiente:

- Levantar inventario de activos de hardware.
- Implementar control de monitoreo de activos de hardware que establezca el tiempo de vida útil restante de los equipos.
- Reemplazar los dispositivos obsoletos o que hayan llegado al fin de su vida útil para eliminar otras vulnerabilidades.

A continuación, se procederá a realizar el análisis de riesgos de los activos de software.

- **Determina vulnerabilidades de inventario de activos de software**
    - Desconocer la cantidad y el estado del software utilizado en la organización puede acarrear problemas de eficiencia, económicos y/o legales.
    - Alojar otras vulnerabilidades digitales en algunos componentes de software utilizado.

.

Tabla 22

Matriz de riesgos de control – Inventario y control de activos de software

MATRIZ DE ANÁLISIS DEL RIESGO																
Vulnerabilidad	**AMENAZA**	**Tipo**		**¿Qué afecta?**			**CONSECUENCIAS**	**Probabilidad**			**Impacto**			**Resultado**	**Riesgo**
		Interna	**Externa**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**0.25**	**0.50**	**0.75**	**0.25**	**0.50**	**0.75**		
Desconocer la cantidad y el estado del software utilizado en la organización puede acarrear problemas de eficiencia, económicos y/o legales.	Caducidad de licencias de uso.	X				X	Imposibilidad de uso del software.	X				X		0.25	MEDIO
	Demanda de fabricantes por uso de licencias	X		X	X	X	Pago de multas por uso de software pirata.	X				X		0.25	MEDIO
Alojar otras vulnerabilidades digitales en algunos componentes de software utilizado.	Alteración de información.	X		X	X	X	Alteración de la información. Imposibilidad de acceder a los datos. Fuga de información.	X					X	0.19	MEDIO
	Existencia de vulnerabilidades	X		X	X	X	Alto riesgo a la disponibilidad, integridad y confidencialidad de la información.		X			X		0.25	MEDIO

Fuente: Maestría de Ciberseguridad UISEK

Elaborado por: Autor

Una vez construida la matriz de riesgos para la falta de inventario y control de activos de software, se puede concluir que en promedio la organización corre un riesgo “medio” en cuanto a amenazas, sin mencionar que los restantes puntos de control se basan en el conocimiento de los activos a proteger, es decir, es importante conocer los dispositivos a proteger.

El plan de tratamiento del riesgo sería el siguiente:

- Levantar inventario de activos de software.
- Implementar control de monitoreo de activos de software.
- Eliminar software no autorizado y/o malicioso.

En el caso de los controles uno y dos, el primer subcontrol de cada uno indica levantar el inventario correspondiente para posteriormente abordar los activos no autorizados, por lo que las actividades planificadas a mayor detalle serán:

  - Elegir software de apoyo para el levantamiento de activos de hardware y software, por lo general estas herramientas permiten llevar el inventario del software de cada uno de los dispositivos reconocidos en la red.
  - Implementar la herramienta de levantamiento de software.
  - Iniciar el proceso de escaneo de la red.
  - Según los resultados del escaneo, se puede completar el inventario con el ingreso manual de los dispositivos no reconocidos automáticamente.
  - Reconocer los dispositivos y software no autorizado.
  - Eliminar de la red los dispositivos que la organización considere innecesario se encuentren conectados a la red.
  - Eliminar el software no autorizado de los dispositivos una vez que la organización determine que no son necesarios para el desarrollo de las actividades.

- Determinar la frecuencia con la cual se realizará un análisis de los activos de hardware y software.

4.4.3. Etapa Proteger

Siguiendo el plan establecido en la etapa de planificación primero se debe levantar el inventario de activos tanto de hardware como de software. Levantar un inventario de activos de hardware y software de forma manual no es nada recomendable, debido a que es fácil perder el control mientras los dispositivos aumentan en la organización, o es posible no considerar activos ocultos a la vista, sin mencionar que de esta forma es imposible poder realizar un monitoreo futuro.

Para solucionar esta problemática, existe herramientas informáticas de escaneo de la red, que permite visualizar todos los equipos conectados a una red informática, existe software simple que permite el escaneo de red o más completos que también analizan el software dentro de cada uno de los dispositivos, adicionalmente proporciona información sobre el hardware instalado dentro de los dispositivos, y en otros casos la herramienta también proporciona el monitoreo en tiempo real de los equipos para evaluar su rendimiento y detectar posibles procesos maliciosos que se ejecuten en segundo plano.

El marco de referencia establece el análisis de dos o más opciones de herramientas informáticas, dentro de estas herramientas se han analizado tres para su implementación dentro de la organización, estas son: Network Inventory Advisor, Spiceworks IT Management Software y Manage Engine Desktop Central.

- **Network Inventory Advisor -** Software que permite realizar el inventario de hardware conectado a la red, y provee información del software instalado en estos dispositivos. Cuenta con una versión de prueba de 15 días y licencia para 25 nodos. Un nodo es cada dispositivo detectado en la red y monitorizado.

Este programa también permite realizar un monitoreo a los dispositivos detectados en la red, donde se puede visualizar los cambios efectuados en el hardware.

- **Spiceworks IT Management Software -** Software Open Source de administración y monitoreo de redes, una de sus primeras funcionalidades es la de manejo de inventario de la red, posee otras características para el monitorio de los dispositivos de la red, necesita de un agente cliente instalado en los dispositivos.
- **Manage Engine Desktop Central -** Software de paga, que permite la gestión de inventario de red, adicional al monitoreo y manejo remoto de los dispositivos, es la herramienta más completa que se ajusta para la implementación del punto de control de manejo y control de inventario de hardware, sin embargo, el valor de su licencia es alto, para estas primeras instancias de la implementación del software de inventario de hardware.

Debido a que no se cuenta con un presupuesto inicial para herramientas de ciberseguridad, se ha elegido en primera instancia el software open source Spiceworks IT Management Software, adicionalmente se ha consultado las calificaciones y opiniones en sitios de análisis de software, como capterra.ec, donde tiene una calificación de 4.4/5 lo que se considera una buena calificación, sin embargo, no se ha cerrado a probar otras ofertas en el mercado, una vez que se ha visualizado por parte de la organización el potencial de este tipo de herramientas.

Por motivos de seguridad y confidencialidad, no se mostrarán los resultados del escaneo de la red con la herramienta seleccionada, sin embargo, se muestra un resumen del inventario de activos en la Tabla 23.

Tabla 23
Tabulación de activos de hardware

Tipo de equipo	Sistema Operativo	Cantidad
Laptop	Windows	37

Laptop	IOS	8
Servidor	Windows Server	4
Servidor	Centos	1
Impresora	Epson	5
Impresora	Aficio Mp	3

Fuente: Autor

En la tabla 24, se muestra un resumen de los activos de software encontrados, por motivos de seguridad y confidencialidad, se ha omitido características más específicas de los programas instalados en los dispositivos.

Tabla 24
Tabulación de activos de software de la empresa

Tipo de software	Proveedor
Software de ofimática	Microsoft
Navegadores de internet	Google/Mozilla/Microsoft
Software de diseño 2D y 3D	Adobe/Trimble
Drivers de dispositivos	Varios

Fuente: Autor

De esta forma se ha podido levantar un primer inventario de activos de hardware y software dentro de la red de la organización.

4.4.3.1. Establecer políticas

La organización ya posee un formato para la elaboración de las políticas de la empresa, estas consisten en los siguientes puntos:

- Objetivo
- Alcance
- Responsable
- Definiciones
- Descripción
- Recomendaciones

De esta forma la política establecida para el punto de inventario y control de activos de hardware es la siguiente:

PO – 122F

POLÍTICA PARA INVENTARIO Y CONTROL DE ACTIVOS DE HARDWARE Y SOFTWARE

1. OBJETIVO

Establecer la gestión del inventario y control de activos de hardware y software dentro de la organización.

2. ALCANCE

Aplica al monitoreo de la red de la oficina matriz y posteriormente a las redes de las sucursales de ventas.

3. RESPONSABLE

Es responsabilidad del departamento de sistemas construir el inventario de activos de hardware y software de la organización y su monitoreo constante.

4. DEFINICIONES

Activo: Recursos necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección.

Hardware: Componente físicos que forman parte de un dispositivo electrónico.

Software: Conjunto de programas y rutinas que permiten a un dispositivo electrónico realizar determinadas tareas.

5. DESCRIPCIÓN

5.1. Registro de activo de hardware y software

Todo dispositivo electrónico que ingrese a la empresa para su uso dentro del desenvolvimiento de las actividades laborales del personal de la

organización debe ser debidamente inventariado, es decir, debe ser registrado las características de este, el custodio que será responsable del mismo, las fechas de ingreso, de alta, mantenimientos y de baja del dispositivo y el software instalado en el mismo.

5.2. Monitoreo de activo de hardware y software

Los activos de hardware y software deben ser monitorizados constantemente, para detectar anomalías funcionales de los dispositivos, tales como degradación de sus componentes de hardware como el consumo anómalo de los recursos del dispositivo.

Una vez se detecte algún tipo de anomalía se debe investigar lo antes posible y en caso de ser necesario informar a quien corresponda del caso suscitado.

5.3. Software de inventario y monitoreo de hardware

El departamento de sistemas es el responsable de adquirir, mantener y gestionar las herramientas que cubran las necesidades del inventario y control de los activos de hardware.

5.4. Detección de intrusos

En caso de detección de activos no correspondientes al inventario de hardware y/o software de la organización, el departamento de sistemas debe bloquear el acceso y de ser posible identificar el activo para su correspondiente registro.

5.5. Bitácora de eventos

El departamento de sistemas debe llevar el registro de todos los eventos anómalos presentados en el monitoreo de activos de hardware, la información

a registrar es: fecha de evento, tipo de evento, descripción del evento, medidas tomadas ante el evento, fecha de cierre del evento.

4.4.4. Etapa Capacitar

Una vez determinado todo el escenario alrededor del punto de control de inventario y control de activos de hardware, se puede establecer que es necesario capacitar tanto en el uso de la herramienta seleccionada como en los procesos a seguir, al personal del departamento de sistemas que se hará cargo del monitoreo de los activos.

Como ya se mencionó en el desarrollo del marco de referencia, el plan de capacitación debe considerar crear conciencia en los usuarios, entrenar habilidades del uso de la herramienta y los procesos establecidos, para de esta forma alcanzar un alto grado de educación en el manejo de inventario de activos de hardware y software.

El plan de capacitación contempla las siguientes actividades:

- Explicación teórica de:
    - Levantamiento de inventario de activos de hardware y software.
    - Vulnerabilidades y riesgos.
    - Importancia de monitoreo de activos de hardware y software.
- Entrenamiento del uso de la herramienta informática.
- Entrenamiento de la aplicación de la política creada con relación al monitoreo de inventario de activos de hardware y software.

De esta forma se da por terminada la implementación del control de seguridad de inventario de activos de hardware y software en la empresa de fabricación, comercialización y exportación de muebles.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Al analizar las normativas vigentes tales como ISO 270001, Nist y CIS en el presente trabajo se pudo evidenciar que el estándar CIS es el más indicado para implementación de controles de seguridad en empresas que se encuentran en una etapa inicial de la gestión de su ciberseguridad, como es el caso de la empresa de fabricación, comercialización y exportación de muebles. CIS clasifica la implementación de los controles según el tamaño y la experiencia de la organización en términos de ciberseguridad, esto ocasiona que la empresa no se sienta abrumada por todo el trabajo que concierne la implementación de los controles, pues la ejecución de estos se lo hace de manera gradual.

- Tras la evaluación concerniente a las medidas de ciberseguridad de la empresa de fabricación, comercialización y exportación de muebles se observó que estas no se encontraban dentro de un plan organizado de ciberseguridad, esto provocó que dichas medidas se encuentren aisladas unas de otras, debido a esto el desarrollo del marco de referencia se centró en otorgar lineamientos simples que faciliten la implementación de controles de ciberseguridad dentro de la empresa.

- El desarrollo del marco de referencia buscó sistematizar el proceso de implementación de controles de seguridad dentro de la empresa de fabricación, comercialización y exportación de muebles, con la finalidad de proteger la información ante cualquier amenaza informática, este marco de referencia se construyó alineado a las pautas establecidas por otras normativas por lo que fácilmente en un futuro se podría adoptar otra normativa según las necesidades de la organización.

- Al definir la aplicación del marco de referencia por fases se aprecia de mejor manera el proceso incremental a seguir al momento de implementar los controles de seguridad, debido a que según se avanza en dicha implementación los últimos controles van dependiendo de la correcta aplicación de los primeros, por lo que es importante en la primera fase conocer lo que se va a proteger.

5.2. RECOMENDACIONES

- Se recomienda a la empresa de fabricación, comercialización y exportación continuar con la implementación de los controles de seguridad informática, hasta completar todos los controles incluidos en el grupo de implementación uno de CIS versión 8, para ello debería contratar al personal calificado para su ejecución.

- La empresa de fabricación, comercialización y exportación debería modificar su organización y contemplar las áreas de seguridad informática, asignar sus roles y funciones para la correcta planificación y ejecución de medidas de seguridad informática a aplicar a largo plazo, más aún ahora que se encuentra en un proceso de expansión organizacional.

- Para futuros trabajos, se recomienda replicar el uso del marco de referencia desarrollada en esta tesis para validar la idoneidad de su aplicación en pequeñas organizaciones que se encuentran iniciando en la implementación de controles de seguridad informática, independientemente de su actividad comercial.

ANEXOS

ANEXO A

Controles CIS Grupo de Implementación 1 (IG1)

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
1				**Inventario y control de activos empresariales**	***Inventariar, rastrear y corregir todos los activos tecnológicos de la empresa conectados a la infraestructura física, virtual, remota y aquellos dentro de entornos de nube, para conocer con precisión la totalidad de los activos que deben monitorearse y protegerse dentro de la empresa. Esto también apoyará la identificación de activos no autorizados para eliminar o remediar.***
1	1,1	Dispositivos	Identificar	Crear y gestionar un inventario detallado de activos empresariales	Crear y gestionar un inventario exacto, detallado y actualizado de todos los activos tecnológicos empresariales con el potencial de almacenar o procesar datos, que incluya: dispositivos de usuario final dispositivos de red, dispositivos no informáticos / IoT y servidores. Se debe asegurar que el inventario registre la dirección de red (si es estática), la dirección física de hardware, el nombre de la máquina, el propietario del activo, el departamento de cada activo y si el activo ha sido aprobado para conectarse a la red. Este inventario incluye activos conectados a la infraestructura física, virtual, remota y dentro de entornos de nube. Además, incluye activos que se conectan regularmente a la infraestructura de red de la empresa, incluso si no están bajo el control de la empresa. Revisar y actualizar el inventario de todos los activos de la empresa semestralmente, o con mayor frecuencia.
1	1,2	Dispositivos	Responder	Abordar activos no autorizados	Asegurar que existe un proceso para abordar los activos no autorizados semanalmente. La empresa puede optar por eliminar el activo de la red, denegar que el activo se conecte de forma remota a la red o poner en cuarentena el activo.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
2				**Inventario y control de activos de software**	***Inventariar, rastrear y corregir todo el software (sistemas operativos y aplicaciones) en la red para que solo se instale y pueda ejecutarse el software autorizado, y que se impida la instalación o ejecución de software no autorizado.***
2	2,1	Aplicaciones	**Identificar**	Crear y gestionar un inventario de software	Establecer y mantener un inventario detallado de todo el software con licencia instalado en los activos de la empresa. El inventario de software debe documentar el título, el editor, la fecha inicial de instalación/ uso y el propósito comercial de cada entrada; cuando corresponda, incluya el Localizador uniforme de recursos (URL), la(s) tienda(s) de aplicaciones, la(s) versión(es), el mecanismo de implementación y la fecha de desmantelamiento. Revise y actualice el inventario de software semestralmente, o con más frecuencia.
2	2,2	Aplicaciones	**Identificar**	Garantizar que el software autorizado sea compatible actualmente	Asegurar que solo el software admitido actualmente se designe como autorizado en el inventario de software para los activos empresariales. Si el software no es compatible, pero es necesario, documente una excepción que detalle los controles de mitigación y la aceptación del riesgo residual. Para cualquier software no compatible sin una documentación de excepción, designe como no autorizado. Revise la lista de software para verificar el soporte de software al menos una vez al mes o con más frecuencia.
2	2,3	Aplicaciones	**Responder**	Abordar software no autorizado	Garantizar que el software no autorizado se elimine del uso en los activos de la empresa o reciba una excepción documentada. Revise mensualmente, o con más frecuencia.
3				**Protección de datos**	***Desarrollar procesos y controles para identificar, clasificar, manejar, retener y eliminar datos de forma segura.***
3	3,1	Datos	**Identificar**	Crear y gestionar un proceso de gestión de datos	Establecer y mantener un proceso de gestión de datos. En el proceso, aborde la sensibilidad de los datos, el propietario de los datos, el manejo de los datos, los límites de retención de datos y los requisitos de eliminación, según los estándares de sensibilidad y retención para la empresa. Actualizar la documentación periódicamente, o cuando se produzcan cambios significativos en la empresa.
3	3,2	Datos	**Identificar**	Establecer y mantener un inventario de datos	Establecer y mantener un inventario de datos, basado en el proceso de gestión de datos de la empresa. Inventario de datos confidenciales, como mínimo. Revise y actualice el inventario anualmente, como mínimo, con prioridad en los datos confidenciales.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
3	3,3	Datos	**Proteger**	Establecer listas de control de acceso a datos	Configurar listas de control de acceso a datos en función de la necesidad de conocimiento de un usuario. Aplique listas de control de acceso a datos, también conocidas como permisos de acceso, a sistemas de archivos, bases de datos y aplicaciones locales y remotos.
3	3,4	Datos	**Proteger**	Aplicar la retención de datos	Conservar los datos de acuerdo con el proceso de gestión de datos de la empresa. La retención de datos debe incluir plazos mínimos y máximos.
3	3,5	Datos	**Proteger**	Elimine los datos de forma segura	Eliminar de forma segura los datos como se describe en el proceso de gestión de datos de la empresa. Asegúrese de que el proceso y el método de eliminación sean proporcionales a la sensibilidad de los datos.
3	3,6	Dispositivos	**Proteger**	Cifrar datos en dispositivos de usuario final	Cifrar los datos en dispositivos de usuario final que contengan datos confidenciales. Las implementaciones de ejemplo pueden incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.
4				**Configuración segura de activos y software**	***Garantizar la configuración segura de los activos empresariales de hardware y software.***
4	4,1	Aplicaciones	**Proteger**	Crear y gestionar un proceso de configuración seguro	Establecer y mantener un proceso de configuración seguro para los activos de hardware y software. Actualizar la documentación periódicamente, o cuando se produzcan cambios significativos en la empresa.
4	4,2	Network	**Proteger**	Establecer y mantener un proceso de configuración seguro para la infraestructura de red	Establecer y mantener un proceso de configuración seguro para los dispositivos de red. Actualizar la documentación periódicamente, o cuando se produzcan cambios significativos en la empresa.
4	4,3	Usuarios	**Proteger**	Configurar el bloqueo automático de sesiones en los activos.	Configurar el bloqueo automático de sesiones en los activos de la empresa después de un período definido de inactividad. Para sistemas operativos de uso general, el período no debe exceder los 15 minutos. Para dispositivos móviles de usuario final, el período no debe exceder los 2 minutos.
4	4,4	Dispositivos	**Proteger**	Implementar y administrar un firewall en servidores	Implementar y administrar un firewall en los servidores, donde sea compatible. Las implementaciones de ejemplo incluyen un firewall virtual, un firewall del sistema operativo o un agente de firewall de terceros.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
4	4,5	Dispositivos	**Proteger**	Implementar y gestionar un firewall en dispositivos de usuario final	Implementar y administrar un firewall basado en host o una herramienta de filtrado de puertos en dispositivos de usuario final, con una regla de prohibición por defecto que elimina todo el tráfico, a excepción de aquellos servicios y puertos que están explícitamente permitidos.
4	4,6	Red	**Proteger**	Gestione de forma segura los activos y el software empresariales	Gestionar de forma segura los activos de hardware y el software de la empresa. Las implementaciones de ejemplo incluyen la administración de la configuración a través de la infraestructura controlada por versiones como código y el acceso a interfaces administrativas a través de protocolos de red seguros, como Secure Shell (SSH) y Hypertext Transfer Protocol Secure (HTTPS). No utilice protocolos de administración inseguros, como Telnet (Red de teletipo) y HTTP, a menos que sea operacionalmente esencial.
4	4,7	Usuarios	**Proteger**	Gestionar cuentas predeterminadas en activos de hardware y software empresariales	Administrar cuentas predeterminadas en activos y software empresariales, como cuentas raíz, de administrador y otras cuentas de proveedor preconfiguradas. Las implementaciones de ejemplo pueden incluir: deshabilitar cuentas predeterminadas o hacerlas inutilizables.
5				**Gestión de cuentas**	***Utilizar procesos y herramientas para asignar y administrar la autorización de credenciales para cuentas de usuario, incluidas cuentas de administrador, así como cuentas de servicio, para activos y software empresariales.***
5	5,1	Usuarios	**Identificar**	Crear y gestionar un inventario de cuentas	Crear y gestionar un inventario de todas las cuentas administradas en la empresa. El inventario debe incluir cuentas de usuario y de administrador. El inventario, como mínimo, debe contener el nombre de la persona, el nombre de usuario, las fechas de inicio / parada y el departamento. Valide que todas las cuentas activas estén autorizadas, de forma trimestral, o con mayor frecuencia.
5	5,2	Usuarios	**Proteger**	Usar contraseñas únicas	Utilizar contraseñas únicas para todos los activos de la empresa. La implementación de prácticas recomendadas incluye, como mínimo, una contraseña de 8 caracteres para las cuentas que usan MFA y una contraseña de 14 caracteres para las cuentas que no usan MFA.
5	5,3	Usuarios	**Responder**	Deshabilitar cuentas inactivas	Eliminar o deshabilitar cualquier cuenta inactiva después de un período de 45 días de inactividad, cuando sea compatible.
5	5,4	Usuarios	**Proteger**	Restringir privilegios de administrador solamente a cuentas de administrador dedicadas	Restringir los privilegios de administrador solamente a las cuentas de administrador dedicadas en los activos de la empresa. Realizar actividades informáticas generales desde la cuenta principal y sin privilegios del usuario.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
6				**Gestión del control de acceso**	***Usar procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos de hardware y software empresariales.***
6	6,1	Usuarios	**Proteger**	Crear un proceso de concesión de acceso	Crear y seguir un proceso, preferiblemente automatizado, para permitir acceso a los activos de la empresa en caso de nueva contratación, concesión de derechos o cambio de rol de un usuario.
6	6,2	Usuarios	**Proteger**	Crear un proceso de revocación de acceso	Crear y siguir un proceso, preferiblemente automatizado, para remover el acceso a los activos de la empresa, mediante la desactivación de cuentas inmediatamente después de la terminación, la revocación de derechos o el cambio de rol de un usuario. Puede ser necesario deshabilitar las cuentas, en lugar de eliminarlas, para preservar las pistas de auditoría.
6	6,3	Usuarios	**Proteger**	Requerir multifactor de autenticación para aplicaciones expuestas externamente	Requerir que todas las aplicaciones empresariales o de terceros expuestas externamente apliquen MFA, donde sea compatible. La aplicación de MFA a través de un servicio de directorio o proveedor de SSO es una implementación satisfactoria de esta Salvaguardia.
6	6,4	Usuarios	**Proteger**	Requerir multifactor de autenticación para el acceso remoto a la red	Requerir multifactor de autenticación para el acceso remoto a la red.
6	6,5	Usuarios	**Proteger**	Requerir multifactor de autenticación para el acceso administrativo	Requerir MFA para todas las cuentas de acceso administrativo, cuando estén admitidas, en todos los activos de la empresa, ya sea administrados in situ o a través de un proveedor externo.
7				**Gestión continua de vulnerabilidades**	***Desarrollar un plan monitorear continuamente las vulnerabilidades en todos los activos dentro de la infraestructura organizacional, con el fin de remediar y minimizar la ventana de oportunidad para los atacantes.***
7	7,1	Aplicaciones	**Proteger**	Crear y gestionar un proceso de gestión de vulnerabilidades	Crear y gestionar un proceso documentado de manejo de vulnerabilidades para los activos empresariales. Actualizar la documentación periódicamente, o cuando se produzcan cambios significativos en la empresa.
7	7,2	Aplicaciones	**Responder**	Crear y gestionar un proceso de corrección	Crear y gestionar una estrategia de remediación basada en el riesgo documentada en un proceso de remediación, con revisiones mensuales o más frecuentes.
7	7,3	Aplicaciones	**Proteger**	Realizar la administración automática de parches del sistema operativo	Realizar actualizaciones del sistema operativo en los activos de la empresa a través de la administración automática de parches mensualmente o con mayor frecuencia.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
7	7,4	Aplicaciones	**Proteger**	Realizar una administración automática de parches de aplicaciones	Realizar actualizaciones de aplicaciones en los activos de la empresa a través de la administración automática de parches mensualmente o con mayor frecuencia.
8				**Gestión de registros de auditoría**	***Recopilar, alertar, revisar y conservar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.***
8	8,1	Red	**Proteger**	Crear y gestionar un proceso de administración de registros de auditoría	Crear y gestionar un proceso de administración de registros de auditoría que defina los requisitos de registro de la empresa. Como mínimo, aborde la recopilación, revisión y retención de registros de auditoría para los activos de la empresa. Actualizar la documentación periódicamente, o cuando se produzcan cambios significativos en la empresa.
8	8,2	Red	**Detectar**	Recopilar registros de auditoría	Recopilar registros de auditoría. Asegúrese de que el registro se haya habilitado en todos los activos de la empresa.
8	8,3	Red	**Proteger**	Garantice un almacenamiento adecuado de registros de auditoría	Asegurar que los destinos de registro mantengan un almacenamiento adecuado para cumplir con el proceso de administración de registros de auditoría de la empresa.
9				**Protecciones de correo electrónico y navegador web**	***Mejorar las defensas y detecciones de amenazas del correo electrónico y los vectores web, ya que estas son oportunidades para que los ciberdelincuentes manipulen el comportamiento humano a través de la participación directa.***
9	9,1	Aplicaciones	**Proteger**	Garantizar el uso de navegadores y clientes de correo electrónico totalmente compatibles	Asegurar que solo los navegadores y clientes de correo electrónico totalmente compatibles puedan ejecutarse en la empresa, utilizando solo la última versión de los navegadores y clientes de correo electrónico proporcionados a través del proveedor.
9	9,2	Red	**Proteger**	Usar servicios de filtrado DNS	Utilizar los servicios de filtrado DNS en todos los activos de la empresa para bloquear el acceso a dominios malintencionados conocidos.
10				**Defensas contra malware**	***Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, código o scripts malintencionados en activos empresariales.***
10	10,1	Dispositivos	**Proteger**	Implementar y mantener software antimalware	Implementar y mantener software antimalware en todos los activos de la empresa.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
10	10,2	Dispositivos	**Proteger**	Configurar actualizaciones automáticas de firmas antimalware	Configurar actualizaciones automáticas para archivos de firma antimalware en todos los activos de la empresa.
10	10,3	Dispositivos	**Proteger**	Deshabilitar la ejecución y la reproducción automáticas para medios extraíbles	Deshabilite la funcionalidad de ejecución automática y ejecución automática para medios extraíbles.
11				**Recuperación de datos**	***Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales dentro del ámbito a un estado previo al incidente y de confianza.***
11	11,1	Datos	**Recuperar**	Establecer y mantener un proceso de recuperación de datos	Establecer y mantener un proceso de recuperación de datos. En el proceso, aborde el alcance de las actividades de recuperación de datos, la priorización de la recuperación y la seguridad de los datos de copia de seguridad. Revisar y actualizar la documentación periódicamente, o cuando se produzcan cambios significativos en la empresa.
11	11,2	Datos	**Recuperar**	Realizar copias de seguridad automatizadas	Realizar copias de seguridad automatizadas de los activos empresariales dentro del ámbito. Ejecutar copias de seguridad semanalmente, o con más frecuencia, en función de la sensibilidad de los datos.
11	11,3	Datos	**Proteger**	Proteja los datos de recuperación	Proteger los datos de recuperación con controles equivalentes a los datos originales. Cifrado de referencia o separación de datos, en función de los requisitos.
11	11,4	Datos	**Recuperar**	Establecer y mantener una instancia aislada de datos de recuperación	Establecer y mantener una instancia aislada de datos de recuperación. Las implementaciones de ejemplo incluyen el control de versiones de destinos de copia de seguridad a través de sistemas o servicios fuera de línea, en la nube o fuera del sitio.
12				**Gestión de la infraestructura de red**	***Establecer, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, para evitar que los atacantes exploten los servicios de red y puntos de acceso vulnerables.***
12	12,1	Red	**Proteger**	Garantizar que la infraestructura de red esté actualizada	Garantizar que la infraestructura de red se mantenga actualizada. Revisar las versiones de software mensualmente, o con más frecuencia, para verificar el soporte de software.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
14				**Conciencia de seguridad y capacitación en habilidades**	***Establecer y mantener un programa de concientización de seguridad para influir en el comportamiento de los empleados, para que crear consciencia en cuanto a la seguridad y se encuentren debidamente capacitados para reducir los riesgos de ciberseguridad para la empresa.***
14	14,1	N/A	**Proteger**	Establecer y mantener un programa de concientización sobre seguridad	El propósito de un programa de concientización de seguridad es educar a la fuerza laboral de la empresa sobre cómo interactuar con los activos y datos de la empresa de manera segura. Realizar capacitación en el momento de la contratación y, como mínimo, anualmente. Revisar y actualizar el contenido anualmente, o cuando se produzcan cambios significativos en la empresa.
14	14,2	N/A	**Proteger**	Capacitar a los colaboradores para que reconozcan los ataques de ingeniería social	Capacitar a los colaboradores en reconocer ataques de ingeniería social, como el phishing.
14	14,3	N/A	**Proteger**	Capacitar a los colaboradores sobre las mejores prácticas de autenticación	Capacitar a los empleados sobre las mejores prácticas de autenticación. Los temas de ejemplo incluyen MFA, composición de contraseñas y administración de credenciales.
14	14,4	N/A	**Proteger**	Capacitar a los colaboradores sobre las mejores prácticas de manejo de datos	Capacitar a los empleados sobre cómo identificar y almacenar, transferir, archivar y destruir adecuadamente los datos confidenciales. Esto también incluye capacitarlos sobre las mejores prácticas de pantalla y escritorio transparentes, como bloquear su pantalla cuando se alejan de su activo empresarial, borrar pizarras físicas y virtuales al final de las reuniones y almacenar datos y activos de forma segura.
14	14,5	N/A	**Proteger**	Capacitar a los colaboradores sobre las causas de la exposición involuntaria a los datos	Capacitar a los colaboradores para que sean conscientes de las causas de la exposición involuntaria a los datos. Los temas de ejemplo incluyen la entrega incorrecta de datos confidenciales, la pérdida de un dispositivo de usuario final portátil o la publicación de datos en audiencias no deseadas.
14	14,6	N/A	**Proteger**	Capacitar a los colaboradores sobre el reconocimiento y la notificación de incidentes de seguridad	Capacitar a los colaboradores para que puedan reconocer un incidente potencial y poder reportar dicho incidente.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
14	14,7	N/A	**Proteger**	Capacite a los colaboradores sobre cómo identificar e informar si sus activos empresariales carecen de actualizaciones de seguridad	Capacitar a los empleados para que comprendan cómo verificar e informar parches de software obsoletos o cualquier falla en procesos y herramientas automatizados. Parte de esta capacitación debe incluir la notificación al personal de TI de cualquier falla en los procesos y herramientas automatizados.
14	14,8	N/A	**Proteger**	Capacite a los colaboradores sobre los peligros de conectarse y transmitir datos empresariales a través de redes inseguras	Capacitar a los empleados sobre los peligros de conectarse y transmitir datos a través de redes inseguras para actividades empresariales. Si la empresa tiene trabajadores remotos, la capacitación debe incluir orientación para garantizar que todos los usuarios configuren de forma segura su infraestructura de red doméstica.
15				**Gestión de proveedores de servicios**	***Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales, o son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.***
15	15,1	N/A	**Identificar**	Crear y gestionar un inventario de proveedores de servicios	Crear y gestionar un inventario de proveedores de servicios. El inventario es para enumerar todos los proveedores de servicios conocidos, incluir clasificaciones y designar un contacto empresarial para cada proveedor de servicios. Actualizar el inventario anualmente, o cuando se produzcan cambios significativos en la empresa.
17				**Gestión de respuesta a incidentes**	***Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes para preparar, detectar y responder rápidamente a un ataque.***
17	17,1	N/A	**Responder**	Designar personal para administrar el manejo de incidentes	Designar a una persona clave, y al menos una copia de seguridad, que administrará el proceso de manejo de incidentes de la empresa. El personal de administración es responsable de la coordinación y documentación de los esfuerzos de respuesta a incidentes y recuperación y puede consistir en empleados internos de la empresa, proveedores externos o un enfoque híbrido. Al utilizar un proveedor externo, designar al menos a una persona interna de la empresa para supervisar cualquier trabajo de terceros. Revisar anualmente, o cuando se produzcan cambios significativos en la empresa.

Control CIS	Salvaguardia CIS	Tipo de Activo	Acción de seguridad	Título	Descripción
17	17,2	N/A	**Responder**	Establecer y mantener la información de contacto para informar incidentes de seguridad	Establecer y mantener la información de contacto de las partes que necesitan ser informadas de incidentes de seguridad. Los contactos pueden incluir personal interno, proveedores externos, fuerzas del orden, proveedores de seguros cibernéticos, agencias gubernamentales relevantes, socios del Centro de Análisis e Intercambio de Información (ISAC) u otras partes interesadas. Verifique los contactos anualmente para asegurarse de que la información esté actualizada.
17	17,3	N/A	**Responder**	Establecer y mantener un proceso empresarial para la notificación de incidentes	Establecer y mantener un proceso empresarial para que la fuerza laboral informe incidentes de seguridad. El proceso incluye el plazo de presentación de informes, el personal al que se debe informar, el mecanismo para la presentación de informes y la información mínima que debe informarse. Asegúrese de que el proceso esté disponible públicamente para toda la fuerza laboral. Revisar periódicamente, o cuando se produzcan cambios significativos en la empresa.

Fuente: CIS Critical Security Controls V8
Traducción: Autor

ANEXO B

FORMATO DE RESUMEN DE ANÁLISIS DE CONTEXTO DE PUNTOS DE CONTROL CIS

FORMATO DE ANÁLISIS DE CONTEXTO DE PUNTOS DE CONTROL CIS				
Punto de control				
Número				
Título				
Objetivo				
Valor agregado				
Resumen de Antecedes				
Implementado	Si		No	
Porcentaje de implementación		%		
Políticas de uso	Si		No	
Documento de la política				
Observaciones de Antecedentes				

Fuente: Autor

ANEXO C

MATRIZ DE RIESGOS

MATRIZ DE ANÁLISIS DEL RIESGO																
Vulnerabilidad	AMENAZA	Tipo		¿Qué afecta?			CONSECUENCIAS	Probabilidad			Impacto			Resultado	Riesgo
		Interna	Externa	Confidencialidad	Integridad	Disponibilidad		0.25	0.50	0.75	0.25	0.50	0.75		

Fuente: Maestría en Ciberseguridad UISEK - Seguridad de datos

REFERENCIAS

Baratta, R., Gobierno de la Ciberseguridad. Ministerio de Industria Comercio y Turismo. España. Recuperado de: https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/ROBERTO%20BARATTA%20MART%C3%8DNEZ.pdf

BASC. (2017). Norma Internacional BASC Sistema de Gestión en Control y Seguridad. BASC. Recuperado de: https://www.bascafe.org/documentos/2019/NORMA%20INTERNACIONAL%20BASC%20V5.pdf

CIS. (2021). CIS Critical Security Controls Version 8. Recuperado de: https://www.cisecurity.org/

Cobb, S. (2019). Guía de Ciberseguridad para Pequeñas Empresas. ESET. Recuperado de: https://www.eset-la.com/pdf/landing/2019/template-leads-b2b/guia-ciberseguridad-pequenas-empresas.pdf

Diligent. (2015). Las cinco mejores prácticas para la gobernanza de la seguridad de la información. Recuperado de: https://diligent.com/wp-content/uploads/2016/10/WP0018_ES_Five-Best-Practices-for-Information-Security-Governance.pdf

Figueroa. J, Rodriguez, R. Bone, C. y Saltos J, (2017). La seguridad informática y la seguridad de la información. Polo del Conocimiento. Recuperado de: https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

Gutiérrez, A. (2013). Magerit: metodología práctica para gestionar riesgos. ESET. Recuperado de: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos

Incibe, (2017). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Incibe, (2017). Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Incibe, (2016). Gestión de riesgos. Una guía de aproximación para el empresario. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

Kaspersky, (2021). Consejos de ciberseguridad para pequeñas empresas: Aspectos básicos. Recuperado de: https://latam.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security

Marchand-Niño, W.-R., & Vega Ventocilla, E. J. (2020). Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS). Interfases, (013), 57-76. Recuperado de: https://doi.org/10.26439/interfases2020.n013.4876

Manage Engine. (2021). ¿Qué son y como implementar los Controles de Seguridad Crítica CIS? Recuperado de: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Maynard, S., Tan, T., Ahmad, A., Ruighaver, T. (2018). Towards a Framework for

Strategic Security Context in Information Security Governance. Pacific Asia Journal of the Association for Information Systems. Recuperado de: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1185&context=pajais

Morales, J. (2017). Riesgos de Ciberseguridad en las Empresas. Universidad Alfonso X El Sabio. Madrid, España. Recuperado de: https://revistas.uax.es/index.php/tec_des/article/view/1174/964

Newmeyer, K. (2015). Ciberespacio, ciberseguridad y ciberguerra. II Simposio Internacional de Seguridad y Defensa. Perú. Recuperado de: https://repositorio.esup.edu.pe/bitstream/20.500.12927/113/1/pp.76-95.pdf

NIST. (2003). Building an Information Technology Security Awareness and Training Program, Computer Security. Technology Administration U.S. Department of Commerce. Estados Unidos. Recuperado de: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Rea-Guaman, M., Calvo-Manzano J. A. y San Feliu T. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas. Universidad Politécnica de Madrid. Boadilla del Monte, Madrid, España. Recuperado de: https://www.researchgate.net/profile/Jose-Calvo-Manzano/publication/326050298_A_prototype_to_manage_cybersecurity_in_small_companies/links/5bb8a3d2299bf1049b7080c6/A-prototype-to-manage-cybersecurity-in-small-companies.pdf

Sistemas de Actuaciones Fiscales (SIAF) (2020). Número de denuncias sobre presuntos delitos informáticos, por año de registro y tipo penal. Periodo 01/01/2015-31/10/2020, Fiscalía General del Estado.