  
**FACULTAD DE ARQUITECTURA E INGENIERÍAS  
Plan de Trabajo de investigación titulado:**

Implementación de controles CIS en la Empresa Tatoo Adventure Gear.

**Realizado por:**

Wágner Alexander Cadena Lastra

**Director del proyecto:**

Ing. Verónica Rodríguez Arboleda, MBA.

Como requisito para la aprobación de la materia:  
DESARROLLO DEL PROYECTO DE INVESTIGACIÓN   
MAESTRÍA EN CIBERSEGURIDAD

QUITO, febrero 2020

# Índice

[Índice 2](#_Toc32950858)

[Índice de Tablas 4](#_Toc32950859)

[Índice de Figuras 5](#_Toc32950860)

[1. Capítulo 1. Introducción 1](#_Toc32950862)

[1.1. Planteamiento del problema 1](#_Toc32950863)

[1.1.1. Diagnóstico. 1](#_Toc32950864)

[1.1.2. Pronóstico. 3](#_Toc32950865)

[1.1.3. Control de pronóstico 4](#_Toc32950866)

[1.1.4. Formulación del problema 5](#_Toc32950867)

[1.2. Objetivos 5](#_Toc32950868)

[1.2.1. Objetivo general 5](#_Toc32950869)

[1.2.2. Objetivos específicos 5](#_Toc32950870)

[1.3. Justificaciones 6](#_Toc32950871)

[1.3.1. Técnica 6](#_Toc32950872)

[1.3.2. Metodológica 7](#_Toc32950873)

[1.4. Marco teórico 8](#_Toc32950874)

[1.4.1. La empresa 8](#_Toc32950875)

[1.4.2. Marcos y estándares de referencia de seguridad 9](#_Toc32950876)

[1.4.3. Confidencialidad, integridad y disponibilidad 10](#_Toc32950877)

[1.4.4. Marco de seguridad cibernética del NIST 11](#_Toc32950878)

[1.4.5. La función del NIST en la Ciberseguridad 12](#_Toc32950879)

[1.4.6. La ISO y su sistema de gobierno 14](#_Toc32950880)

[1.4.7. Los controles del CIS 15](#_Toc32950881)

[1.5. Marco Conceptual 16](#_Toc32950882)

[1.6. Estado del arte. 17](#_Toc32950883)

[1.6.1. Taxonomías 17](#_Toc32950884)

[1.6.2. Métricas 18](#_Toc32950885)

[1.6.3. Arquitecturas de referencia 18](#_Toc32950886)

[1.7. Adopción de una perspectiva teórica 20](#_Toc32950887)

[2. Método 20](#_Toc32950888)

[2.1. Estudio del problema 20](#_Toc32950889)

[2.2. Modalidad de la investigación 21](#_Toc32950890)

[2.3. Método 21](#_Toc32950891)

[3. Aspectos Administrativos 21](#_Toc32950892)

[3.1. Recursos humanos 21](#_Toc32950893)

[3.2. Recursos técnicos y materiales. 22](#_Toc32950894)

[3.3. Recursos financieros 24](#_Toc32950895)

[3.4. Cronograma de trabajo 1](#_Toc32950896)

[3.5. Índice o temario preliminar 1](#_Toc32950897)

[**Bibliografías** 3](#_Toc32950898)

[4. Anexos 1](#_Toc32950899)

[4.1. Encuesta del estado del área de sistemas aplicada al Helpdesk 1](#_Toc32950900)

[4.2. Principios y prácticas de CIS RAM 5](#_Toc32950901)

[4.2.1. Principios 5](#_Toc32950902)

[4.2.2. Prácticas 5](#_Toc32950903)

[4.2.3. Pasos para la evaluación de riesgos 5](#_Toc32950904)

[4.3. Manual de análisis de riesgos, una introducción 8](#_Toc32950905)

[4.4. Bases en Derecho y Regulación 8](#_Toc32950906)

[4.5. ¿Vale la pena este análisis extendido? En pocas palabras, sí. 11](#_Toc32950907)

[4.6. Tipo de estudio 11](#_Toc32950908)

[4.6.1. Nivel de evaluación de riesgos 11](#_Toc32950909)

[4.6.2. Elección de una perspectiva de ciberseguridad 13](#_Toc32950910)

[4.7. Definiendo el Alcance físico 13](#_Toc32950911)

[4.8. Programación de sesiones de entrevista 14](#_Toc32950912)

[4.9. Programación de revisiones de evidencia 15](#_Toc32950913)

# Índice de Tablas

[Tabla 1: Crecimiento de población institucional. 4](#_Toc32950914)

[Tabla 2: Crecimiento de Ventas por año 4](#_Toc32950915)

[Tabla 3:Comparación de los primeros cinco controles del CIS con el ISO 27001:2013 y COBIT. fuente: (CIS Critical Security Controls Team, 2016) 10](#_Toc32950916)

[Tabla 4: Matriz de Madurez de Critical Security Controls Initial Assessment Tool (v6.1c) fuente: (Center for Internet Security, 2019) 18](#_Toc32950917)

[Tabla 5: Alineación de principios y prácticas de RAM de CIS a la ley, regulaciones y estándares de seguridad - Anexo 3.2. 9](#_Toc32950918)

[Tabla 7: Alcance de activos de empresa. 14](#_Toc32950919)

[Tabla 8: Plan de proyecto para implementación. 15](#_Toc32950920)

# Índice de Figuras

[Figure 1: Estructura de la cadenas de valor de la empresa modelo de Retail, como se puede ver el área de tecnología es parte de toda la cadena y por lo tanto aporta en casi todas las áreas de la empresa. 8](#_Toc32950921)

[Figure 2: Mapa de relación de NIST y del CIS, fortaleciendo la arquitectura fuente: . 20](#_Toc32950922)

[Figure 3: Captura de sitio CIS CSAT, aquí se llenara los datos obtenido en las encuestas y ayudará al manejo de requisitos y tiempos fuente: (Chris Cronin. Partner, HALOCK Security Labs, 2018). 23](#_Toc32950923)

[Figure 4: Sistema Online EcuaTask, es un CMDB (Configuration Management Data Base) adaptado para pequeñas empresas. Fuente: https://devinventario.ecuatask.com/home 23](#_Toc32950924)

[Figure 5: Captura de Sistema que alimenta la configuración del equipo al sistema EcuaTask y ayuda a generar el levantamiento de líneas bases y a enumerar el software instalado en el sistema. Fuente: https://github.com/wcadena/ecuatask-desktop 24](#_Toc32950925)

[Figure 6: Captura de monitor Nagios en el cual se monitorea equipos y servicios. 24](#_Toc32950926)

[Figure 7: Tabla de costos estimados consultada en base a costos del mercado. Fuente: Costo de sistema: Codecanion, Dominio: DigitalOcean y Godaddy, Nagios: Freelancer, Respaldos: GoogleOne, Nomina: Tatoo. 25](#_Toc32950927)

[Figure 8: Cronograma Propuesto de trabajo para aplicación de la tesis. Fuente: investigador. 1](#_Toc32950928)

# 

## Capítulo 1. Introducción

## Planteamiento del problema

### Diagnóstico.

Tatoo Adventure Gear ha crecido durante el último año incorporando a sus servicios dos nuevas innovaciones de negocios, una de ellas es el mejoramiento de su sitio web y la segunda, la ampliación del catálogo de servicios con la incorporación de paquetes turísticos que se pueden contratar en un sitio web independiente y dedicado.

No se ha realizado una auditoría de sistemas y de seguridad en los últimos tres años, por lo que ahora se desea conocer el estado del área informática y cuáles son las oportunidades de desarrollo potenciales, que por la falta de documentación están ocultos.

El área de sistemas cuentan con procedimientos, los cuales ahora no son suficientes, y las reglas de antivirus se pueden complementar con políticas de usuarios, esta es una oportunidad de mejora importante.

Es menester que al crecer las empresas busquen facilidades para conocer, catalogar y planificar el manejo de sus activos tecnológicos, el manejo de contabilidad sobre los activos generalmente incluye información de la fecha de compra, importante para el manejo de devaluación, modelos y proveedores, relevante para las garantías y el código contable, importante para el momento de realizar un levantamiento contable, sin embargo, ninguno de estos datos ayudan al saber si estos activos están aportando al cambio tecnológico, o si se están cumpliendo las normativas sobre el uso de licencias o si se está aprovechando al 100% los equipos que tiene la empresa. (Stalling, 2017)

Una de las responsabilidades del equipo de Helpdesk se centran en la protección de los sistemas electrónicos, y la primordial garantía de seguridad en la que confían se centra en el antivirus, pero no se toma en cuenta la seguridad física al momento de crear una protección general a los riesgos de la organización, las paredes, cerraduras son un factor importante en la seguridad, pero no es suficiente, políticas, control de inventarios, control de software y control de permisos son necesarios. (Stalling, 2017)

En contraste, es más fácil enseñarle a un ingeniero informático o eléctrico las bases de la seguridad física que a otra persona con un grado de capacitación diferente enseñarle bases de seguridad digital, razón por la cual las interacciones entre la protección física y lógica generalmente dependen de la persona de sistemas para administrar.

Ahora se debe tener en cuenta que muchos mecanismos de seguridad de la información pueden ser derrotados sin la necesidad de la intervención física de un “chico malo” ya sea en el desarrollo, durante el envío o la instalación de software, ya que un usuario bien intencionado podría “Sin querer” dar acceso a la infraestructura o a datos de la empresa al instalar un programa no catalogado y que puede tener vulnerabilidades.

Además, la empresa entiende que dar facilidades a los usuarios para que conecten sus equipos particulares a la red y puedan comunicarse con proveedores, compañeros y familiares por medio de la tan galopante nueva mensajería como es WhatsApp les da tranquilidad, ahorro y con un nuevo concepto que es el salario emocional, sin embargo, esto genera un nuevo reto al equipo de sistemas ya que deben determinar cuáles equipos deben tener acceso y cuales pertenecen a la organización y cuáles no.

Se ha realizado una auditoría y la observación directa muestran que la organización no cuenta con un manual de políticas de tecnologías, tampoco manual de procedimientos de tecnología ni planes de contingencia, y existen brechas en la seguridad tales como:

* La organización no tiene un sistema de Directorio Activo, que permita implementar controles óptimos para gestionar el acceso y el uso controlado de los recursos de la red de datos corporativa.
* A pesar de que la organización ha implementado un antivirus corporativo debidamente licenciado, existen equipos que no están protegidos con esta herramienta.
* Existen usuarios que no hacen uso del bloqueo de pantallas en los ordenadores asignados, esto permite que cualquier persona pueda acceder a ellos cuando el usuario se ausenta de su lugar de trabajo.
* Las credenciales de las cuentas de correos electrónicos de los usuarios son conocidas por los administradores de tecnología.
* No existe puerta metálica ni panel biométrico en el acceso al centro de cómputo.
* Se evidencia que existe una deficiencia con el control de acceso a periféricos como USB, esto permitiría la infección del equipo por malware o la sustracción de información.
* No existen convenios de confidencialidad para las personas que ocupan cargos críticos en donde se establezcan cláusulas de no divulgación de información de la organización.
* El área de tecnología no posee una política de seguridad informática donde se detallen los lineamientos y responsabilidades para el tratamiento seguro de la información, poniendo en riesgo a la confidencialidad, integridad y disponibilidad de esta.

### Pronóstico.

Tatoo Adventure Gear ha determinado como parte de su estrategia institucional la innovación dentro del área deportiva, optimizando su catálogo de servicios e invirtiendo en Innovación y desarrollo (I+D), debido a esta nueva estrategia es importante considerar como prioridad la seguridad de la información, que es uno de los activos valiosos que garantizan continuidad del negocio y sostenibilidad a la organización.

Tabla 1: Crecimiento de población institucional.

|  |  |  |
| --- | --- | --- |
| Año | Cantidad de ingresos de usuarios por año. | Crecimiento del personal al año. |
| 2015 | 3 | 30 |
| 2016 | 2 | 32 |
| 2017 | 2 | 34 |
| 2018 | 3 | 37 |
| 2019 | 3 | 40 |

Fuente: Área de contabilidad Tatoo.

Tabla 2: Crecimiento de Ventas por año

|  |  |
| --- | --- |
| Año | Porcentaje de incremento en ventas |
| 2015 | 45 |
| 2016 | 55 |
| 2017 | 59 |
| 2018 | 62 |
| 2019 | 63 |

Fuente: Área de Ventas y Marketing.

Como se puede observar la cantidad de ventas y de usuarios ha tenido un crecimiento importante para la empresa, de la mano de este aumento de equipos también han incrementado el software, causando el cambio de la infraestructura incluso de ubicación de las oficinas, esto naturalmente ha elevado los requerimientos de seguridad en el área de Helpdesk, siendo imprescindible la implementación de controles de seguridad a la medida, el objetivo es evitar en lo posible daños, la pérdida de reputación de la empresa, pérdidas económicas y afectación de productividad. (Chris Cronin. Partner, HALOCK Security Labs, 2018)

### Control de pronóstico

Se necesita colocar un conjunto de controles sin afectar la eficiencia o el grado de colaboración, mejorando la utilidad y productividad optimizando los fondos y recursos pertinentes, la alta directiva ha determinado que desea una solución de seguridad informática, pero sin que el tiempo que se dedique a ello retrase los lanzamientos de Innovación y desarrollo, tampoco que consuma los recursos asignados a las principales prioridades de innovación y que tampoco signifique incrementos en los costos, así que se va a planear usar una herramienta que se adapte a esta necesidad inicial.

Se hace necesario proporcionar un método para evaluar el riesgo mediante el cálculo de la probabilidad de un impacto para la empresa, los clientes, los objetivos comerciales y las entidades externas (reguladores, proveedores, etc.). y que se mantenga en el marco de lo que se va a denominar como riesgo aceptable, el cual generará un plan de “seguridad razonable” (Chris Cronin. Partner, HALOCK Security Labs, 2018).

CIS RAM proporciona un método para "trazar una línea" en la definición de riesgo aceptable de una organización, con riesgos por debajo de la línea que se adhieren a la atención debida y riesgos por encima de la línea que requieren tratamiento de riesgo.

### Formulación del problema

Mediante la información recopilada y los procesos de auditoría realizados en el área tecnológica de Tatoo Adventure Gear se ha encontrado brechas en la seguridad de la información, esto puede afectar a los procesos de tecnología de la organización y posibles pérdidas de información, económicas, reputación de la empresa y afectación de productividad.

## Objetivos

### Objetivo general

Implementar controles de ciberseguridad en las oficinas de Ecuador de la empresa Tatoo Adventure Gear mediante la aplicación de las seis primeras acciones fundamentales sugeridas por el CENTER FOR INTERNET SECURITY que garantice la confidencialidad, integridad y disponibilidad de la información.

### Objetivos específicos

* Identificar la situación actual de la infraestructura tecnológica e informática de la empresa Tatoo Adventure Gear en la sede de Ecuador, mediante la aplicación de una matriz de riesgos que permita el análisis de las vulnerabilidades y amenazas que está expuesta.
* Analizar el nivel de seguridad que se debe aplicar a la empresa Tatoo Adventure Gear en las oficinas de Ecuador mediante la aplicación de encuestas y entrevistas que permita la identificación del grado de personalización que se va a aplicar a los controles de ciberseguridad.
* Determinar los controles de seguridad que se aplicarán a Tatoo Adventure Gear sede Ecuador mediante el análisis de los indicadores de la CIS-RAM que permitan la mitigación de las vulnerabilidades encontradas~~.~~
* Aplicar los controles seleccionados de la CIS en la empresa Tatoo Adventure Gear de las cede Ecuador para atenuar los riesgos asociados con las amenazas de seguridad de la información existentes.

## Justificaciones

### Técnica

La información es el nuevo activo más importante para la empresa, ahora, el primer paso para tener segura la inversión que se ha realizado es saber qué es lo que se debe asegurar, el levantamiento de activos físicos y de datos facilitará enumerar las prioridades entre lo que se debe dar mayor o menor ponderación al asegurar la información, se debe tener en cuenta que esta generación de prioridades debe estar conectada con los intereses de la operación y del negocio (National Institute of Standards and Technology | NIST, 2019).

En la actualidad la empresa Tatoo Adventure Gear cuenta con 40 empleados (Tabla 1: Crecimiento de población institucional.) los cuales cuentan a su haber al menos una computadora como custodios, pero según datos capturados en la encuesta al área de Sistemas (Anexo 1) ninguno cuenta con una política de uso, o una acta de entrega de activos o un acta de responsabilidad ante su manipulación.

De la información recolectada se puede observar que Tatoo Adventure Gear posee riesgos asociados a la seguridad de la información, esto debido a la falta de políticas y procedimientos, también se ha notado que los activos no se encuentran asignados a un responsable y que los usuarios pueden ejecutar aplicaciones como administradores poniendo su equipo e información en riesgo.

### Metodológica

En los últimos años se ha hecho evidente que, en el mundo de la seguridad de la información, el delito supera a la defensa. A pesar de que los presupuestos aumentan y la administración presta más atención a los riesgos de pérdida de datos y penetración del sistema, los datos aún se pierden y los sistemas aún se están penetrando. Una y otra vez las personas preguntan: "¿Qué podemos hacer prácticamente para proteger nuestra información?". La respuesta ha llegado en la forma de 20 controles de garantía de información conocidos como los Controles CIS. (Center for Internet Security, 2019)

*Critical Security Controls* se enfoca primero en priorizar las funciones de seguridad que son efectivas contra las últimas amenazas dirigidas avanzadas, con un fuerte énfasis en "Lo que funciona": controles de seguridad donde se utilizan productos, procesos, arquitecturas y servicios que han demostrado efectividad en el mundo real. La estandarización y la automatización son otra de las principales prioridades, para obtener eficiencias operativas y al mismo tiempo mejorar la efectividad. Las acciones definidas por los Controles son demostrablemente un subconjunto del amplio catálogo definido por el Instituto Nacional de Estándares y Tecnología (NIST) SP 800-53. Los Controles no intentan reemplazar el trabajo del NIST, incluido el Marco de Seguridad Cibernética desarrollado en respuesta a la Orden Ejecutiva 13636. En cambio, los Controles priorizan y se centran en un número menor de controles accionables con altos beneficios, con el objetivo de una filosofía "debe hacer primero". Dado que los Controles se derivaron de los patrones de ataque más comunes y se examinaron en una comunidad muy amplia de gobierno e industria, con un consenso muy fuerte sobre el conjunto resultante de controles, sirven como base para una acción inmediata de alto valor.

El método de evaluación de riesgos CIS es un método gratuito de estimación de peligros de seguridad de la información que ayuda a las organizaciones a implementar y evaluar su postura de seguridad frente a las mejores prácticas de seguridad cibernética de Controles de CIS y CIS RAM proporciona instrucciones, ejemplos, plantillas y ejercicios para realizar una evaluación de riesgos cibernéticos

## Marco teórico

### La empresa

Después de revisar el informe de empresarial que se divulgó en abril del 2019 (Corporación Favorita, 2019), se puede afirmar que la seguridad de la información no es uno de los ejes en los cuales la corporación está centrada en este momento, sin embargo, la mejora continua es una de las prioridades en los que se desea trabajar y fortalecer.

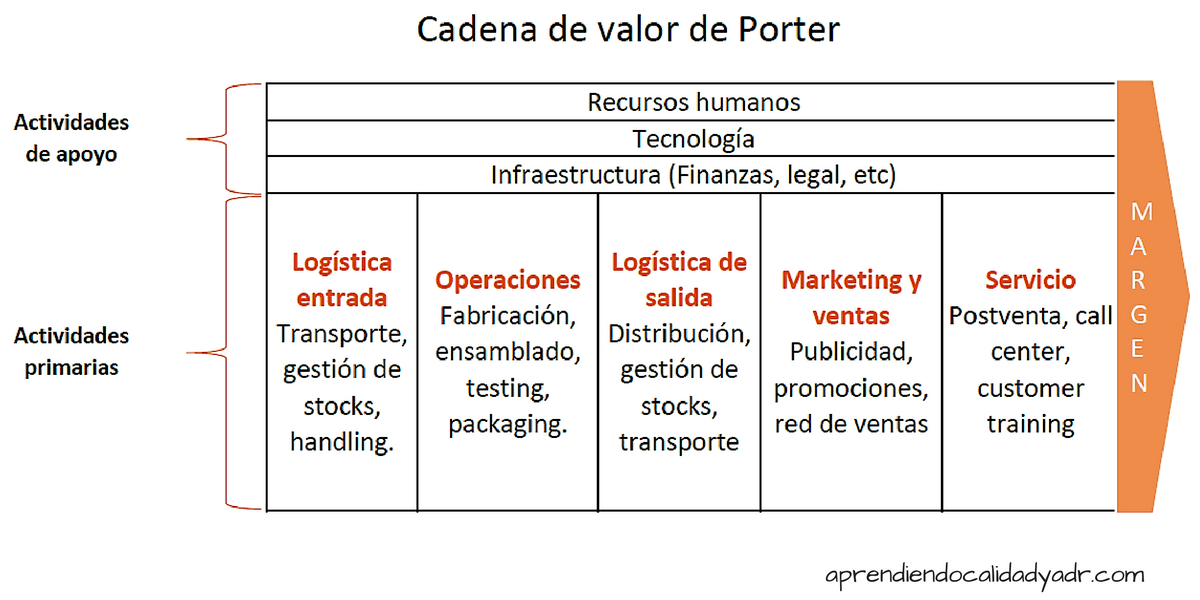


Figure 1: Estructura de la cadenas de valor de la empresa modelo de Retail, como se puede ver el área de tecnología es parte de toda la cadena y por lo tanto aporta en casi todas las áreas de la empresa.

Todas las partes de la empresa se pueden abstraer como tabiques de la ventaja competitiva, la eficiencia y la calidad son las actividades fundamentales, buscan las mejores metodologías aplicables a sus actividades comerciales y productivas, después de analizar las cantidades de usuarios con equipos tecnológicos, se puede afirmar que más del 80% de usuarios tiene acceso a uno.

Actualmente la ciberseguridad ha generado mucha expectativa en las empresas, debido a al aumento de inversiones en activos informáticos, por lo que poco a poco se ha mejorado la perspectiva de la alta gerencia a los pilares de la seguridad informática, confiabilidad, integridad y disponibilidad, es por eso que Tatoo Adventure Gear a considerado oportunamente la implementación de controles a la medida para garantizar la continuidad del negocio.

### Marcos y estándares de referencia de seguridad

Una serie de organizaciones públicas y privadas, incluida la Organización Internacional de Normalización (ISO) y el Instituto Nacional de Normas, Estándares y Tecnología (NIST), han invertido mucho tiempo y energía para desarrollar normas que permitan marcos de ciberseguridad proactivos. Se va a analizar los estándares desarrollados por ambas organizaciones. Antes de comenzar a construir nuestro programa y políticas de seguridad de la información, primero debemos identificar qué se debe lograr y por qué. Comencemos por lo tanto discutiendo los tres principios básicos de la seguridad de la información. Luego se considerara la creciente amenaza global, que incluye quién está detrás de los ataques, su motivación y cómo atacan. Se puede aplicar este conocimiento para construir el marco de nuestro programa de seguridad de la información y cómo redactamos nuestras políticas.

Dentro del estándar a usar se describen los primeros cinco controles críticos de seguridad del CIS, los cuales corresponden a los primeros pasos que se tomarán para implementar seguridad en la empresa, los controles a control comparado con el ISO 27002:2013 y COBIT

Tabla 3:Comparación de los primeros cinco controles del CIS con el ISO 27001:2013 y COBIT.  
fuente: (CIS Critical Security Controls Team, 2016)

|  |  |  |
| --- | --- | --- |
| Control crítico de seguridad | ISO 27002:2013 | COBIT 5 |
| Control de seguridad crítico n. ° 1: inventario de dispositivos autorizados y no autorizados | A.8.1.1 A.9.1.2 A.13.1.1 | APO13: Gestionar seguridad  DSS05: Gestionar servicios de seguridad  BAI09: Gestionar activos |
| Control de seguridad crítico n. ° 2: inventario de software autorizado y no autorizado | A.12.5.1 A.12.6.2 | APO13: Gestionar seguridad  DSS05: Administrar servicios de seguridad |
| Control de seguridad crítico n. ° 3: configuraciones seguras para hardware y software | A.14.2.4 A.14.2.8 A.18.2.3 | APO13: Gestionar seguridad  DSS05: Gestionar servicios de seguridad  BAI10: Gestionar configuración |
| Control de seguridad crítico n. ° 4: evaluación y corrección continua de vulnerabilidades | A.12.6.1 A.14.2.8 | APO13: Gestionar seguridad  DSS05: Administrar servicios de seguridad |
| Control de seguridad crítico # 5: uso controlado de privilegios administrativos | A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4 | APO13: Gestionar seguridad  DSS05: Administrar servicios de seguridad |

### Confidencialidad, integridad y disponibilidad

Los elementos de confidencialidad, integridad y disponibilidad a menudo se describen como el modelo de la CIA (Stalling, 2017). Es fácil adivinar que lo primero que se le ocurrió cuando leyó esas tres cartas fue la Agencia Central de Inteligencia de los Estados Unidos. En el mundo de la ciberseguridad, estas tres letras representan algo que se debe conseguir, lograr y proteger. La confidencialidad, integridad y disponibilidad (*Confidentiality, Integrity, Availability* - *CIA*) son los atributos unificadores de un programa de seguridad de la información. En conjunto, denominado tríada de la *CIA* o modelo de seguridad de la *CIA*, cada atributo representa un objetivo fundamental de la seguridad de la información.

Ahora, después de leer esta pequeña introducción se produce una pregunta: ¿Quién es responsable de la *CIA*? Es responsabilidad de los propietarios de la información garantizar la confidencialidad, integridad y disponibilidad. ¿Qué significa ser propietario de información? Según FISMA, el propietario de la información es un funcionario con autoridad legal u operativa para la información específica y la responsabilidad de establecer los criterios para su creación, recopilación, procesamiento, difusión o eliminación, que pueden extenderse a sistemas interconectados o grupos de sistemas interconectados (Ross, Swanson , Stoneburner, Katzke , & Johnson, 2004). Más simplemente, el propietario de la información tiene la autoridad y la responsabilidad de garantizar que la información esté protegida, desde la creación hasta la destrucción.

Los departamentos de tecnología de la información (TI) o sistemas de información (SI) son ampliamente percibidos como propietarios de los sistemas de información e información. Quizás esto se deba a que la palabra "información" es parte del título del departamento. Para el registro, con la excepción de la información específica de su departamento, los departamentos de TI e IS no deben considerarse propietarios de la información. Más bien, son las personas encargadas de mantener los sistemas que almacenan, procesan y transmiten la información. Se les conoce como custodios de la información: los responsables de implementar, mantener y monitorear las salvaguardas y los sistemas. Son más conocidos como administradores de sistemas, webmasters e ingenieros de redes (Terán, 2014).

### Marco de seguridad cibernética del NIST

Antes de discutir el Marco de seguridad cibernética del NIST en detalle, se propondrá un marco de seguridad. El marco de seguridad es un término colectivo dado a la orientación sobre temas relacionados con la seguridad de los sistemas de información, principalmente en relación con la planificación, implementación, gestión y auditoría de prácticas generales de seguridad de la información. Uno de los marcos más completos para la ciberseguridad es el NIST *Cybersecurity Framework*, La guía del NIST sobre la confiabilidad de los sistemas cubre varias áreas técnicas. Estas áreas incluyen orientación general sobre ciberseguridad, computación en la nube, *bigdata* y sistemas físicos. Estos esfuerzos y orientación se centran en los objetivos de seguridad de confidencialidad, integridad y disponibilidad (CIA).

### La función del NIST en la Ciberseguridad

Fundada en 1901, NIST es una agencia federal no regulada dentro de la Administración de Tecnología del Departamento de Comercio de EE. UU. La misión de NIST es desarrollar y promover medidas, estándares y tecnología para mejorar la productividad, facilitar el comercio y mejorar la calidad de vida (NIST Team, 2017). La División de Seguridad Informática (CSD) es una de las siete divisiones dentro del Laboratorio de Tecnología de la Información del NIST. La misión del CSD de NIST es mejorar la seguridad de los sistemas de información de la siguiente manera:

* Al crear conciencia sobre los riesgos de TI, las vulnerabilidades y los requisitos de protección, particularmente para las tecnologías nuevas y emergentes.
* Investigando, estudiando y asesorando a las agencias sobre las vulnerabilidades de TI y diseñando técnicas para la seguridad y la privacidad rentables de los sistemas federales sensibles.
* Desarrollando estándares, métricas, pruebas y programas de validación
* para promover, medir y validar la seguridad en sistemas y servicios,
* educar a los consumidores y establecer requisitos mínimos de seguridad para los sistemas federales.
* Desarrollando una guía para aumentar la planificación, implementación, administración y operación de TI segura (NIST Team, 2017).

La Ley de Gobierno Electrónico de 2002 (Congress, 2002) asignó al NIST la misión de desarrollar un Marco de Garantía de la Información (normas y directrices) diseñado para sistemas de información federales que no están designados como sistemas de seguridad nacional de Estados Unidos de Norteamérica. El Marco de Garantía de Información del NIST incluye los Estándares Federales de Procesamiento de Información (FIPS) y Publicaciones Especiales (SP). Aunque desarrollado para uso gubernamental, el marco es aplicable al sector privado y aborda los aspectos administrativos, operativos y técnicos de la protección de la CIA de la información y los sistemas de información (NIST Team, 2017).

El NIST define la seguridad de la información como la protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar CIA.

Actualmente, hay más de 500 documentos relacionados con la seguridad de la información del NIST. Este número incluye FIPS, la serie SP 800, información, boletines del Laboratorio de Tecnología de la Información (ITL) e informes inter agencias NIST (NIST IR):

* Normas federales de procesamiento de información (FIPS): esta es la serie de publicaciones oficiales de normas y directrices.
* Serie 800 de Publicación Especial (SP): Esta serie informa sobre la investigación, las directrices y los esfuerzos de divulgación de ITL en la seguridad del sistema de información y sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas (National Institute of Standards and Technology | NIST, 2019).
* Publicación especial (SP) de la serie 1800: esta serie se centra en las prácticas y pautas de seguridad cibernética (National Institute of Standards and Technology | NIST, 2019).
* Informes internos o interinstitucionales del NIST (NISTIR): estos informes se centran en los resultados de la investigación, incluida la información de antecedentes para FIPS y SP.
* Boletines de ITL: cada boletín presenta una discusión en profundidad de un solo tema de gran interés para la comunidad de sistemas de información. Los boletines se emiten según sea necesario. Desde los controles de acceso hasta la seguridad inalámbrica, las publicaciones del NIST son realmente un tesoro de valiosa y práctica guía.

### La ISO y su sistema de gobierno

ISO es una red de institutos de normas nacionales de más de 164 países. Cada país miembro tiene permitido un delegado, y una Secretaría Central en Ginebra, Suiza, coordina el sistema. En 1946, delegados de 25 países se reunieron en Londres y decidieron crear una nueva organización internacional, cuyo objetivo sería "facilitar la coordinación internacional y la unificación de las normas industriales". La nueva organización, ISO, comenzó oficialmente a operar el 23 de febrero de 1947. ISO es una organización no gubernamental. A diferencia de las Naciones Unidas, sus miembros no son delegaciones de gobiernos nacionales. Sin embargo, ISO ocupa una posición especial entre los sectores público y privado. Esto se debe a que, por un lado, muchos de sus institutos miembros son parte de la estructura gubernamental de sus países, o están obligados por su gobierno (International Organization for Standardization, 2019).

Por otro lado, otros miembros tienen sus raíces únicamente en el sector privado, ya que fueron creados por asociaciones nacionales de asociaciones industriales. ISO ha desarrollado más de 13,000 estándares internacionales en una variedad de temas, que van desde códigos de país hasta seguridad de pasajeros.

La serie ISO / IEC 27000 comprende estándares de seguridad de la información publicados conjuntamente por ISO y la Comisión Electrotécnica Internacional (IEC). Los primeros seis documentos de la serie ISO / IEC 27000 proporcionan recomendaciones para "establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información". En total, hay 22 documentos en la serie, y varios más Todavía están en desarrollo.

* ISO 27001 es la especificación para un Sistema de gestión de seguridad de la información (SGSI). • ISO 27002 describe el Código de prácticas para la gestión de la seguridad de la información.
* ISO 27003 proporciona una guía de implementación detallada. • ISO 27004 describe cómo una organización puede monitorear y medir la seguridad utilizando métricas.
* ISO 27005 define el enfoque de gestión de riesgos de alto nivel recomendado por ISO.
* ISO 27006 describe los requisitos para las organizaciones que medirán el cumplimiento de ISO 27000 para la certificación.

El marco es aplicable a organizaciones públicas y privadas de todos los tamaños. Según el sitio web de ISO, “el estándar ISO ofrece recomendaciones para la gestión de la seguridad de la información para uso de quienes son responsables de iniciar, implantar o mantener la seguridad en su organización. Su objetivo es proporcionar una base común para desarrollar estándares de seguridad organizacionales y prácticas efectivas de administración de seguridad y proporcionar confianza en los tratos entre organizaciones”.

### Los controles del CIS

Conocidos como (CIS CONTROLS) es un conjunto de mejores prácticas de defensa para mitigar los ataques más comunes contra sistemas y redes, estos controles son desarrollados por un grupo de expertos en TI que aplican su experiencia en ciberseguridad para crear estas mejores prácticas de seguridad que es aceptada globalmente, estos expertos provienen de varios sectores que incluyen ventas al por menor, fabricación, salud, educación, gobierno, defensa y otros.

## Marco Conceptual

**Apropiado**: Una condición en la cual los riesgos para los activos de información no crearán previsiblemente un daño que sea mayor de lo que la organización o las partes interesadas pueden tolerar (Center for Internet Security, 2019).

**Clase de activo**: Un grupo de activos de información que se evalúan como un conjunto en función de su similitud. "Servidores", "computadoras de usuario final", "dispositivos de red" son ejemplos, como son "servidores de correo electrónico", "servidores web" y "servidores de autenticación" (Center for Internet Security, 2019).

**Carga**: El impacto negativo que una salvaguarda puede representar para la organización, o para otros (Center for Internet Security, 2019).

**Control**: un método documentado para proteger los activos de información mediante salvaguardas técnicas, físicas o de procedimiento (Center for Internet Security, 2019).

**Impacto**: el daño que puede sufrir cuando una amenaza compromete un activo de información (Center for Internet Security, 2019).

**Puntuación de impacto**: la magnitud del impacto que puede sufrir. Esto se establece en lenguaje sencillo y está asociado con escalas numéricas, generalmente de '1' a '3' o '1' a '5' (CIS TEAM, 2020).

**Tipo de impacto**: una categoría de impacto que estima la cantidad de daño que puede afectar a una parte o un propósito. La RAM CIS describe tres tipos de impacto; Misión, objetivos y obligaciones (ISO 27001 , 2005).

**Activo de información**: información o los sistemas, procesos, personas e instalaciones que facilitan el manejo de la información (ISO 27001 , 2005).

**Riesgo inherente**: la probabilidad de que ocurra un impacto cuando una amenaza compromete un activo desprotegido (ISO 27001 , 2005).

**Probabilidad**: el grado en que se espera que una amenaza genere un impacto. Puede expresarse en términos de frecuencia, previsibilidad o probabilidad (Center for Internet Security, 2019).

**Medida**: Una indicación repetible y basada en evidencia de que una salvaguarda logra su objetivo de control (Center for Internet Security, 2019).

**Riesgo observado**: El riesgo actual tal como le parece al evaluador de riesgos (Center for Internet Security, 2019).

**Riesgo residual**: el riesgo que queda después de aplicar una salvaguarda. CIS RAM no utiliza directamente este concepto, pero implica que el riesgo se reduce cuando se aplica una protección. El riesgo residual no tiene en cuenta los posibles impactos negativos para la organización cuando se aplican las salvaguardas (Center for Internet Security, 2019).

**Riesgo**: una estimación de la probabilidad de que una amenaza cree un impacto no deseado. En términos de este método, el riesgo puede expresarse como el producto de una probabilidad y un impacto.

## Estado del arte.

A continuación, se examinaran y analizaran el estado del arte relacionado con las métricas de seguridad en general.

### Taxonomías

El objetivo de la taxonomía es definir, armonizar y agrupar los conceptos en una clasificación internacionalmente acordada ,Estándares existentes como ISO 27001 (ISO 27001 , 2005). es una iniciativa en curso que hasta ahora no ha propuesto ninguna nueva taxonomía o métrica de alto nivel. También promueve la Matriz de controles de la, que se basa El NIST (National Institute of Standards and Technology | NIST, 2019) y propone una serie de preguntas que proporcionan requisitos de seguridad fundamentales para guiar y evaluar riesgo general de seguridad. Todas estas propuestas se consolidan de manera práctica por la aportada por el Centro de Seguridad de Internet (CIS). Ambas son bastante similares acerca de las categorías definidas y el conjunto propuesto de definiciones métricas. Debido a su flexibilidad, creemos que las métricas propuestas en ambos documentos también se pueden aplicar a empresa a través de taxonomías.

### Métricas

El CIS ha creado una plantilla que caracteriza cada métrica con atributos, y también ha propuesto sus primeras 40 métricas que cubren cinco de los primeros controles críticos de seguridad. Esta metodología (CIS TEAM, 2020) propone un conjunto de parámetros de seguridad y resistencia que pueden evaluar los procesos y estado de seguridad de la empresa. Los parámetros propuestos se dividen en categorías de alto nivel (preparación, prestación de servicios, respuesta, recuperación, cumplimiento legal y regulatorio) así:

Tabla 4: Matriz de Madurez de Critical Security Controls Initial Assessment Tool (v6.1c)  
fuente: (Center for Internet Security, 2019)

|  |  |
| --- | --- |
| Nivel de Madurez | Descripción: |
| Nivel uno | Políticas completas |
| Nivel dos | Controles 1-5 implementados |
| Nivel tres | Todos los controles implementados |
| Nivel cuatro | Todos los controles automatizados |
| Nivel cinco | Todos los controles reportados |

En particular con la definición de esta "plantilla" métrica flexible que al ayuda para crear métricas más específicas que sean objetivas y cuantitativas. (CIS Critical Security Controls Team, 2016)

### Arquitecturas de referencia

Elija marcos que guíen el trabajo de su programa de seguridad y, en última instancia, simplifiquen el complejo mundo de la ciberseguridad de una manera que los líderes empresariales puedan entender más fácilmente.

• Los marcos de control describen los controles de seguridad que son la base de cada programa de seguridad.

• Los marcos del programa ayudan a estructurar el programa de seguridad, establecer una base para evaluar las actividades del programa y simplificar la comunicación sobre el programa.

• Los marcos de riesgo proporcionan un enfoque consistente para administrar y evaluar el riesgo de una manera que proporcione valor al negocio.

Elija un marco de cada una de estas tres categorías para madurar su programa con el tiempo. Los ejemplos de marcos comunes incluyen:

* + Marcos de control
    - NIST 800-53
    - Controles CIS
  + Marcos de programa
    - ISO 27001
    - NIST CSF
  + Marcos de riesgo
    - NIST 800-39, 800-37, 800-30
    - ISO 27005
    - CIS RAM
    - JUSTA.

Los tres marcos de seguridad se pueden usar juntos. Tenemos una muestra cómo los Controles CIS pueden asignarse a las Categorías y Funciones del Marco de Seguridad Cibernética (CSF) del NIST.

|  |  |  |
| --- | --- | --- |
| FUNCIÓN | CATEGORÍA | CIS CONTROL |
| Identificar | • Gestión de activos | CIS Control #1, 2 |
|  | • Ambiente de negocios |  |
|  | • Gobierno |  |
|  | • Evaluación de riesgos | CIS Control #3 |
|  | • Estrategia de gestión de riesgos |  |
|  | • Gestión de riesgos de la cadena de suministro |  |
| Detectar | • Gestión de identidad, autenticación y control de acceso. | CIS Control # 4 |
|  | • Conciencia y entrenamiento | CIS Control #4 |
|  | • Seguridad de datos | CIS Control #1, 2 |
|  | • Procesos y procedimientos de protección de la información. | CIS Control #3, 5 |
|  | • mantenimiento | CIS Control #4 |
|  | • Tecnología protectora | CIS Control # 4 |
| Proteger | • Monitoreo continuo de seguridad | CIS Control #3 |
| Responder | • Análisis | CIS Control #3 |
|  | • Mitigación | CIS Control #3 |

Figure 2: Mapa de relación de NIST y del CIS, fortaleciendo la arquitectura  
fuente: . (Center for Internet Security, 2019)

## Adopción de una perspectiva teórica

CIS RAM proporciona tres conjuntos de instrucciones que describen un proyecto completo de evaluación de riesgos. Cada conjunto de instrucciones está diseñado para organizaciones con diferentes capacidades de gestión de seguridad de la información para aumentar la utilidad del método.

# Método

## Estudio del problema

En relación a los objetivos planteados el tipo de estudio que se propondrá es Exploratorio, ya que no se tiene un punto inicial para partir con toma de datos, usaremos como base lo propuesto principalmente en la matriz de CIS.

Una de las razones principales de usar el tipo de estudio exploratorio es por la razón que no se tiene un modelo propio a seguir sobre políticas, debido a que usar el ISO 27000 podría resultar muy complicado y extenso, así como el NIST podría solicitar puntos de control que no se acercan a la realidad latinoamericana, es por eso que es necesidad generar un punto de partida y según a la información que se obtendrá crear un propio grupo controles que cubran los más importante del marco elegido (Center for Internet Security, 2019).

## Modalidad de la investigación

Debido que el investigador tiene acceso directo a las áreas a las que se va evaluar y que la disponibilidad de personal en la empresa es limitada la metodología a usar es de campo.

## Método

La investigación contará con encuestas y entrevistas que seguirán el marco sugerido en el CIS RAM, la facilidad con la que se cuenta es que parte del equipo a entrevistar tienen al menos 7 años como parte del equipo y con un máximo de 15 años en la misma empresa, después de explicar las bondades decidieron aportar con su conocimiento y completar los datos requeridos, esto sumando al plan del CIS nos ayudará a ir colocando uno a uno los controles que se adapten al negocio, esta descripción se adapta al método histórico lógico, como ya explicamos la toma de datos cuenta con la experiencia del equipo y la aplicación del marco ajustado a las necesidades del negocio complementaran el método lógico, ya que no se adaptara o aplicará controles que no fuesen necesarios como la aplicación de un Dominio, ya que por el momento no se tiene la madurez interna para aplicarlo y no se cuenta con el personal o los recursos en este momento, sin embargo se pueden colocar controles que compensen esto y que se mantengan dentro del Marco de implementación.

# Aspectos Administrativos

## Recursos humanos

El equipo interno de la empresa es un equipo multidisciplinario, sin embargo, está separada la mayoría del proceso a encargados que se les ha designado una labor y que se encargan de realizarla, esta estructura se suele mostrar dentro del estudio de los recursos humanos y administrativos como estructuras familiares (Bringas, 2018), sus beneficios suelen ser:

* Trato familiar
* Relación con jefes y dueños
* Poca o ninguna burocracia
* Rapidez en las decisiones

Y justamente esto es lo que vamos a aprovechar para facilitar la investigación, ya que la toma de decisiones se facilita al tener de primera mano las aprobaciones necesarias del caso.

Para la investigación vamos a definir 4 perfiles principales:

1. Investigador. - Este perfil corresponde al Asesor de Ciberseguridad, el cual estará en la mayoría de las etapas guiando al resto de las personas y tiene conocimientos sobre Tecnológicas de la información y comunicaciones, además de conceptos claros sobre Integridad, Disponibilidad y Confidencialidad. (Chris Cronin. Partner, HALOCK Security Labs, 2018)
2. Gerencia. – Es la persona encargada en la toma de decisiones, es el responsable al cual tiene la posibilidad de toma de medidas independientes sin aprobación mayor (Chris Cronin. Partner, HALOCK Security Labs, 2018).
3. Ejecutivo. – Es un especialista en el área correspondiente, toma decisiones con un alcance, asesora a Gerencia (Chris Cronin. Partner, HALOCK Security Labs, 2018).
4. Personal. – Es parte de la empresa, está en contacto directo con la operación, cuenta con un manual de operaciones u objetivos que limitan su toma de decisiones, es un experto en las tareas asignadas, depende de un ejecutivo o gerencia (Chris Cronin. Partner, HALOCK Security Labs, 2018).

## Recursos técnicos y materiales.

Se usará para la evaluación las siguientes herramientas:

* Herramienta en línea CIS SAT
  + Esta herramienta ayudará al levantamiento de datos, su direccione es: https:// csat.cisecurity.org/
  + Solo se puede ingresar con un perfil administrador.

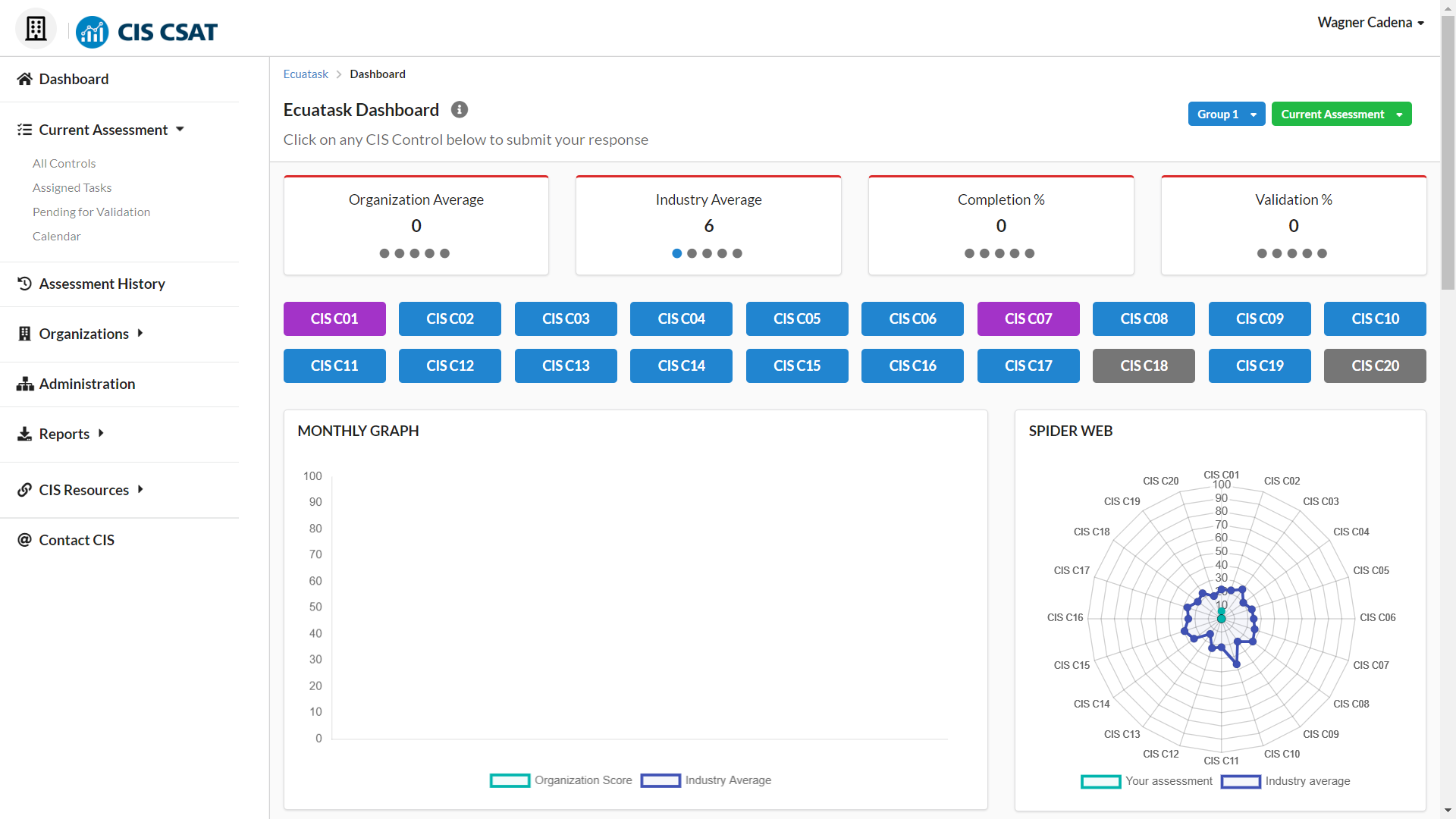


Figure 3: Captura de sitio CIS CSAT, aquí se llenara los datos obtenido en las encuestas y ayudará al manejo de requisitos y tiempos  
fuente: (Chris Cronin. Partner, HALOCK Security Labs, 2018).

* Excel de evaluación con controles generales del CIS RAM (Chris Cronin. Partner, HALOCK Security Labs, 2018).
* Para el levantamiento de los datos de equipos, software y generar actas de entrega e historial de mantenimiento se usará:
  + Sistema Online EcuaTask de inventarios.

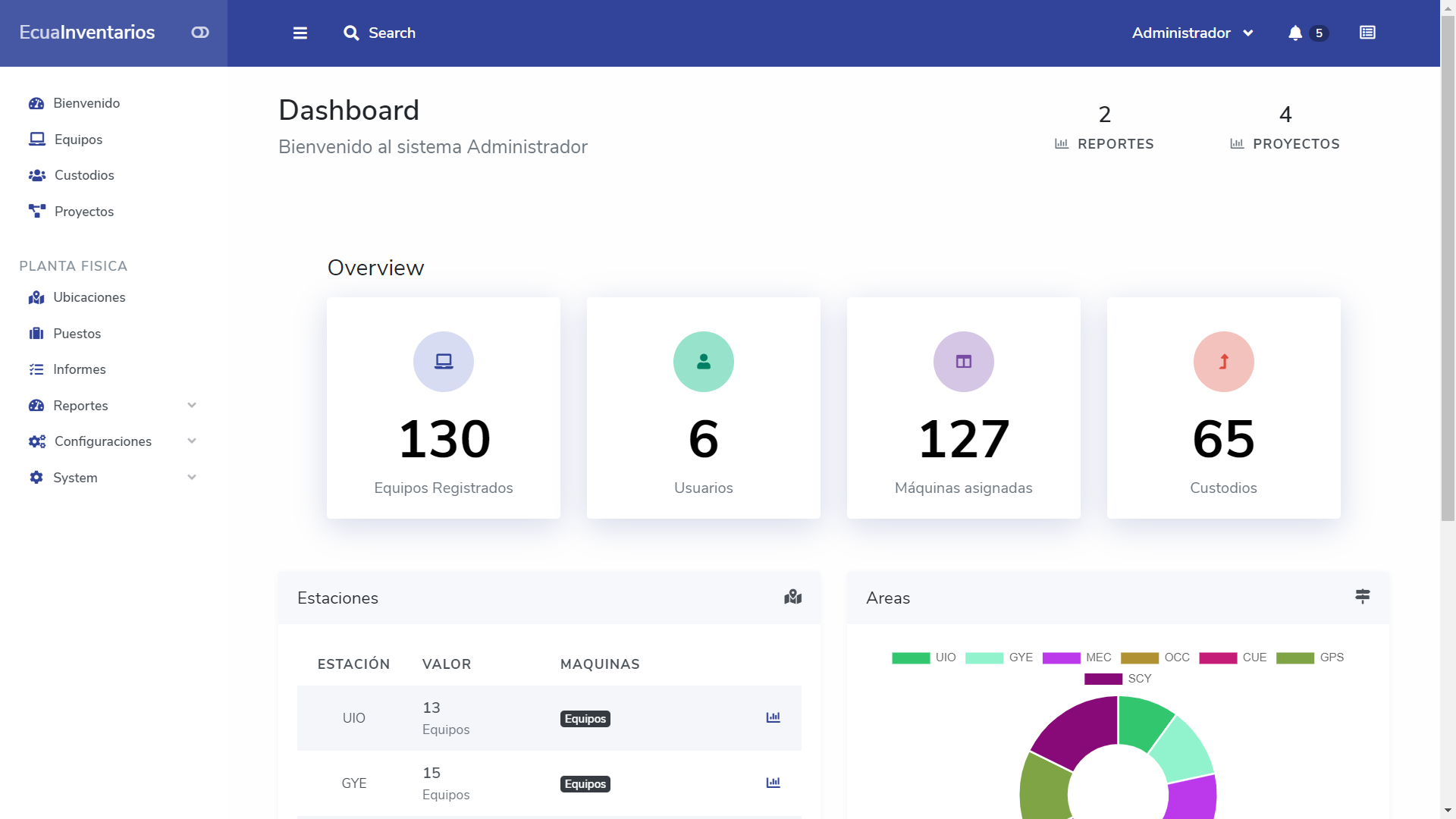


Figure 4: Sistema Online EcuaTask, es un CMDB (Configuration Management Data Base) adaptado para pequeñas empresas.  
Fuente: <https://devinventario.ecuatask.com/home>

* + Para la alimentación de los datos de Software y configuraciones de Equipos de escritorio se usará la herramienta EcuataskDesktop

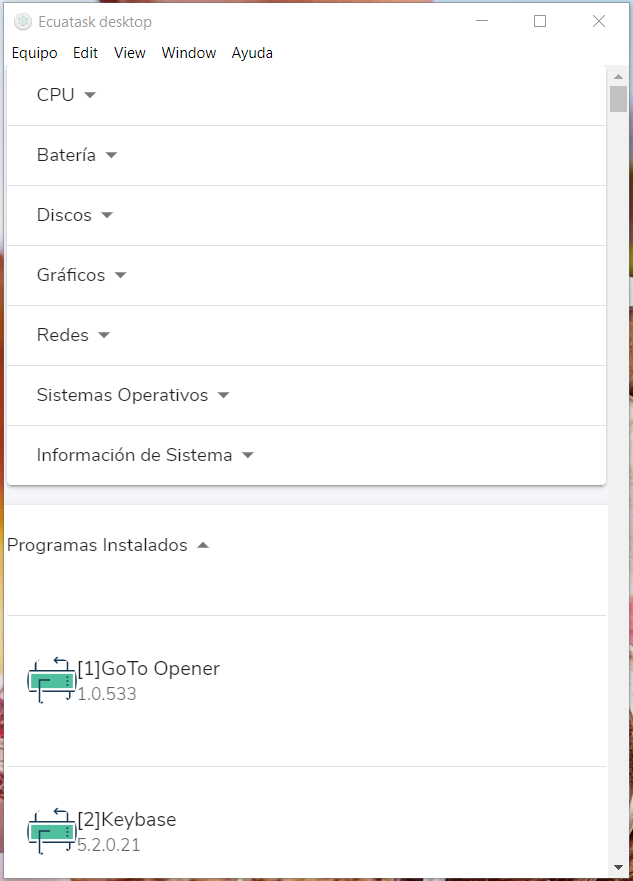


Figure 5: Captura de Sistema que alimenta la configuración del equipo al sistema EcuaTask y ayuda a generar el levantamiento de líneas bases y a enumerar el software instalado en el sistema.  
Fuente: <https://github.com/wcadena/ecuatask-desktop>

* + Para el monitoreo de los equipos y servicios se usará Nagios Core.

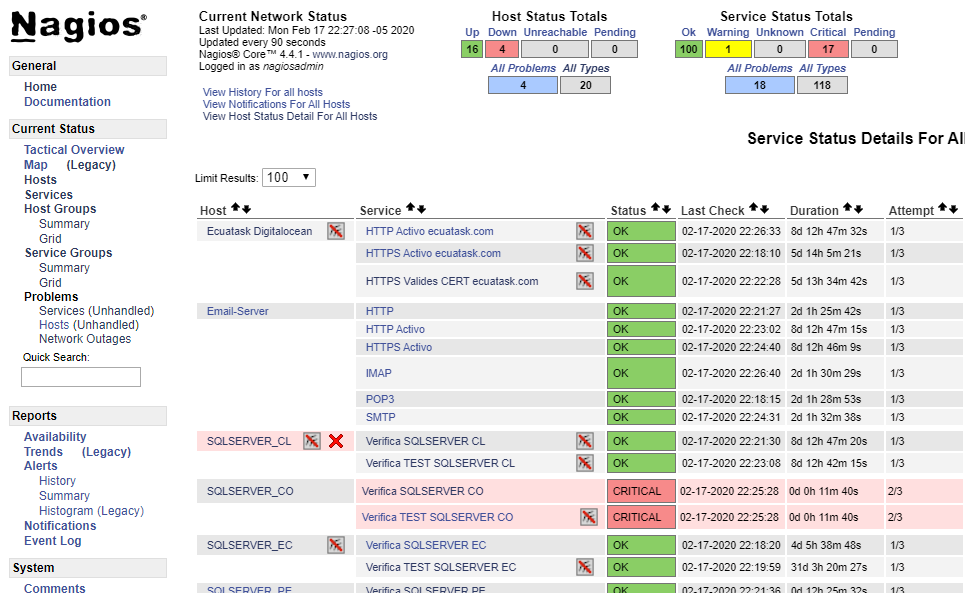


Figure 6: Captura de monitor Nagios en el cual se monitorea equipos y servicios.

Fuente: Monitor Nagios Tatoo.

* + NSClient es un agente diseñado originalmente para trabajar con Nagios, se instalará sólo en los equipos a ser monitoreados.

## Recursos financieros

Para esta investigación se necesitará:

|  |  |  |  |
| --- | --- | --- | --- |
| # | Descripción | Costo Anual | Financiación |
| 1 | Sistema Ecuatask | $250 | Investigador |
| 2 | Host dominio | $72 | Investigador |
| 3 | Dominio | $17 | Investigador |
| 4 | Sistema EcuataskDesktop | $250 | Investigador |
| 5 | Sistema Nagios | $250 | Investigador |
| 6 | Instalación de Cliente NSCliente | $220 | Investigador |
| 7 | Configuración de Nagios | $300 | Investigador |
| 8 | Respaldos Online | $24 | Investigador |
| 9 | Mano de Obra ($7,5 /Hora) |  | Tatoo / Investigador. |
| Total | | $1359 |  |

Figure 7: Tabla de costos estimados consultada en base a costos del mercado.  
Fuente: Costo de sistema: Codecanion, Dominio: DigitalOcean y Godaddy, Nagios: Freelancer, Respaldos: GoogleOne, Nomina: Tatoo.

## Cronograma de trabajo

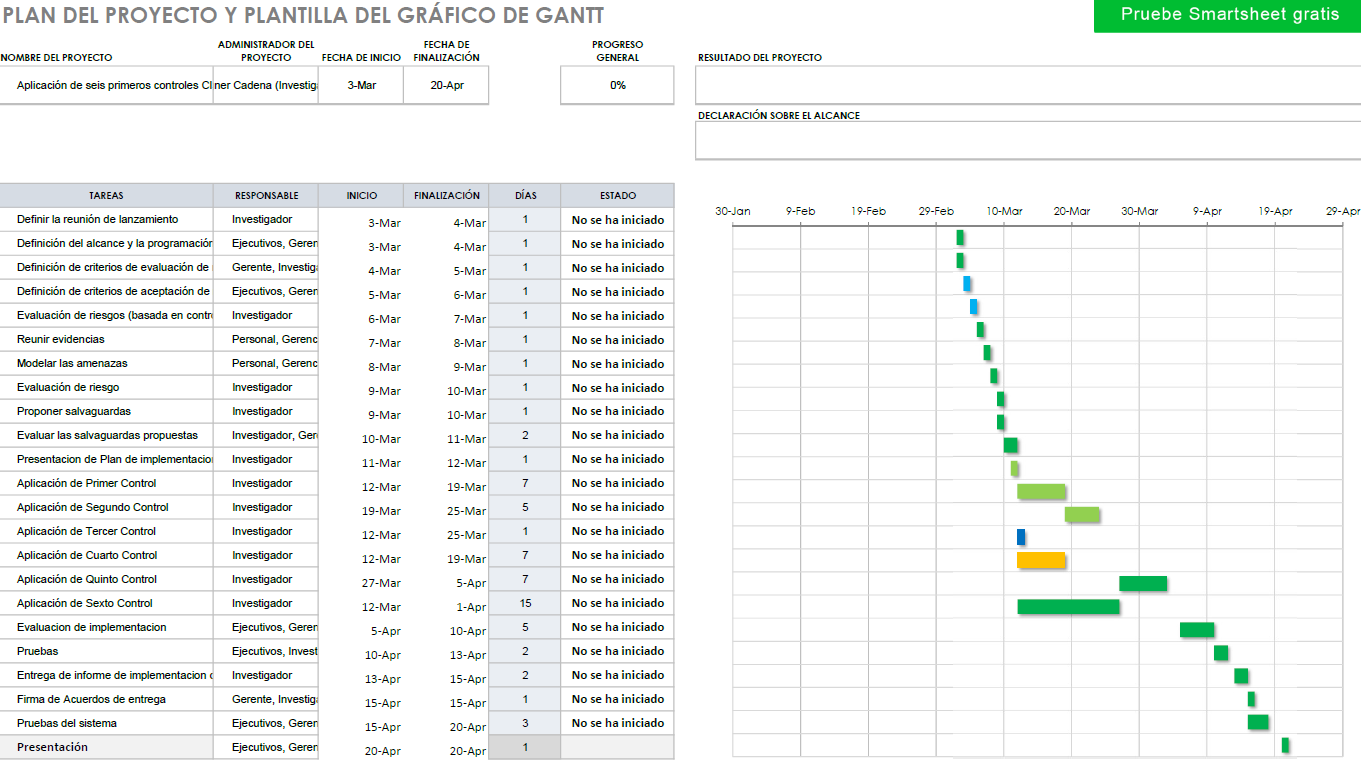


Figure 8: Cronograma Propuesto de trabajo para aplicación de la tesis. Fuente: investigador.

## Índice o temario preliminar

Se propone el siguiente índice para el desarrollo de la investigación:

|  |  |  |  |
| --- | --- | --- | --- |
| Nivel 1 | Nivel 2 | Nivel 3 | Índice de Investigación |
| 1 |  |  | Capítulo 1. |
| 1 |  |  | Introducción |
| 1 | 1 |  | Planteamiento del problema |
| 1 | 2 |  | Diagnóstico. |
| 1 | 3 |  | Pronóstico. |
| 1 | 4 |  | Control de pronóstico |
| 1 | 5 |  | Formulación del problema |
| 1 | 6 | 1 | Objetivos |
| 1 | 6 | 2 | Objetivo general |
| 1 | 6 | 3 | Objetivos específicos |
| 1 | 7 |  | Justificaciones |
| 1 | 8 |  | Técnica |
| 1 | 9 |  | Metodológica |
| 2 |  |  | Capítulo 2 |
| 2 | 1 |  | Marco teórico |
| 2 | 1 | 1 | La empresa |
| 2 | 1 | 2 | Marcos y estándares de referencia de seguridad |
| 2 | 1 | 3 | Confidencialidad, integridad y disponibilidad |
| 2 | 1 | 4 | Marco de seguridad cibernética del NIST |
| 2 | 1 | 5 | La función del NIST en la Ciberseguridad |
| 2 | 1 | 6 | La ISO y su sistema de gobierno |
| 2 | 1 | 7 | Los controles del CIS |
| 2 | 2 |  | Marco Conceptual |
| 2 | 3 |  | Estado del arte. |
| 2 | 3 | 1 | Taxonomías |
| 2 | 3 | 2 | Métricas |
| 2 | 3 | 3 | Arquitecturas de referencia |
| 2 | 3 | 4 | Adopción de una perspectiva teórica |
| 3 |  |  | Capítulo 3. |
| 3 | 1 |  | Situación Actual |
| 3 | 2 |  | Descripción Técnica |
| 3 | 3 |  | Análisis de riesgo actual |
| 3 | 4 |  | Criterios de evaluación de riesgos |
| 3 | 5 |  | Criterios de aceptación de riesgos |
| 3 | 6 |  | Evaluación de riesgos |
| 3 | 6 | 1 | Resultado de Mediciones iniciales |
| 3 | 7 |  | Modelar las amenazas |
| 3 | 8 |  | Evaluación de riesgo |
| 3 | 9 |  | Salvaguardas propuestas |
| 3 | 10 |  | Mapa de controles CIS |
| 4 |  |  | Capítulo 4. |
| 4 | 1 |  | Propuesta |
| 4 | 2 |  | Alcance de la propuesta |
| 4 | 3 |  | Evaluación de riesgos para la empresa |
| 4 | 4 |  | Identificación y selección de controles CIS |
| 4 | 5 |  | Plan de implementación |
| 4 | 5 | 1 | Primer Control |
| 4 | 5 | 2 | Segundo Control |
| 4 | 5 | 3 | Tercer Control |
| 4 | 5 | 4 | Cuarto Control |
| 4 | 5 | 5 | Quinto Control |
| 4 | 5 | 6 | Sexto Control |
| 4 | 6 |  | Resultado de Mediciones Finales |
| 5 |  |  | Capítulo 5. |
| 5 | 1 |  | Conclusiones |
| 5 | 2 |  | Recomendaciones |
| 5 | 3 |  | Bibliografía |
| 6 |  |  | Anexos |

**Bibliografías**

Bringas, M. L. (2018). *Protocolos en Empresas Familiares.* Madrid: Unión Editorial.

Center for Internet Security. (2019). *CIS Controls V7.* East Greenbush: Center for Internet Security.

Chris Cronin. Partner, HALOCK Security Labs. (2018). *CIS RAM Express Edition - Center for Internet Security Risk Assessment Method (Version 1.0).* East Greenbush: Center for Internet Security.

CIS Critical Security Controls Team. (01 de 10 de 2016). *CIS Critical Security Controls - Center for Internet Security*. Obtenido de Mappings to the CIS Critical Security Controls: https://www.cisecurity.org/wp-content/uploads/2017/03/Poster\_Winter2016\_CSCs.pdf

CIS TEAM. (16 de 02 de 2020). *CIS CSAT*. Obtenido de CIS controls: https://csat.cisecurity.org/

Congress. (2002). *PUBLIC LAW 107–347—DEC. 17 2002.* Washington: Congress.

Corporación Favorita. (2019). *Informe Anual Corporación Favorita.* Quito: Imprenta Mariscal. Obtenido de https://issuu.com/corporacionfavorita/docs/informe\_cf\_2019\_

International Organization for Standardization. (23 de 11 de 2019). *ABOUT US*. Obtenido de ISO - International Organization for Standardization: https://www.iso.org/about-us.html

ISO 27001 . (2005). *ISO/IEC 27001 Español ed.* Madrid: ISO.

National Institute of Standards and Technology | NIST. (23 de 11 de 2019). *National Institute of Standards and Technology | NIST*. Obtenido de COMPUTER SECURITY RESOURCE CENTER: https://csrc.nist.gov/publications/sp800

National Institute of Standards and Technology | NIST. (23 de 11 de 2019). *National Institute of Standards and Technology | NIST*. Obtenido de COMPUTER SECURITY RESOURCE CENTER: https://csrc.nist.gov/publications/sp1800

NIST Team. (14 de 06 de 2017). *About NIST*. Obtenido de National Institute of Standards and Technology: https://www.nist.gov/about-nist

Ross, R., Swanson , M., Stoneburner, G., Katzke , S., & Johnson, A. (2004). *Guide for the Security Certification and Accreditation of Federal Information Systems NIST Special Publication 800-37.* Gaithersburg: NIST Special Publication.

Stalling, W. (2017). *Network Security Essentials Aplications and Standards.* Hoboken: Pearson.

Terán, D. (2014). *Administración Estratégica de la Función Informática.* México: Alfaomega.

Velthuis, M. P., del Peso, E., & del Peso, M. (2008). *Auditoría de tecnologías y de sistemas de información.* Madrid: Alfaomega Ra-Ma.

# Anexos

## Encuesta del estado del área de sistemas aplicada al Helpdesk

|  |  |  |  |
| --- | --- | --- | --- |
| *Código* | *Pregunta* | *Aplica* | *Si / NO* |
| *CARNÉ DE IDENTIDAD* | Desarrollar una comprensión organizacional para administrar el riesgo de ciberseguridad para los sistemas, las personas, los activos, los datos y las capacidades. |  |  |
| *ID.AM* | Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización lograr los propósitos comerciales se identifican y gestionan de manera coherente con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización. | Aplica | NO |
| *ID.AM-1* | Se inventarían dispositivos y sistemas físicos dentro de la organización | Aplica | Si |
| *ID.AM-2* | Se inventarían las plataformas y aplicaciones de software dentro de la organización. | Aplica | No |
| *ID.AM-3* | La comunicación organizacional y los flujos de datos se mapean | No | No |
| *ID.AM-4* | Los sistemas de información externos están catalogados | APLICA | NO |
| *ID.AM-5* | Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial. |  |  |
| *ID.AM-6* | Se establecen roles y responsabilidades de ciberseguridad para toda la fuerza laboral y los terceros interesados ​​(por ejemplo, proveedores, clientes, socios) |  |  |
| *SERÍA* | La misión, los objetivos, las partes interesadas y las actividades de la organización se entienden y priorizan; Esta información se utiliza para informar las funciones de seguridad cibernética , las responsabilidades y las decisiones de gestión de riesgos. |  |  |
| *ID.BE-1* | Se identifica y comunica el papel de la organización en la cadena de suministro. |  |  |
| *ID.BE-2* | Se identifica y comunica el lugar de la organización en la infraestructura crítica y su sector industrial. |  |  |
| *ID.BE-3* | Se establecen y comunican las prioridades para la misión, los objetivos y las actividades de la organización. |  |  |
| *ID.BE-4* | Se establecen dependencias y funciones críticas para la prestación de servicios críticos. |  |  |
| *ID.BE-5* | Los requisitos de resistencia para respaldar la prestación de servicios críticos se establecen para todos los estados operativos (por ejemplo, bajo coacción / ataque, durante la recuperación, operaciones normales) |  |  |
| *ID.GV* | Las políticas, procedimientos y procesos para administrar y monitorear los requisitos reglamentarios, legales, de riesgo, ambientales y operativos de la organización se entienden e informan a la administración del riesgo de ciberseguridad. |  |  |
| *ID.GV-1* | Se establece y comunica la política de ciberseguridad organizacional. |  |  |
| *ID.GV-2* | Las funciones y responsabilidades de ciberseguridad están coordinadas y alineadas con funciones internas y socios externos. |  |  |
| *ID.GV-3* | Los requisitos legales y reglamentarios relacionados con la ciberseguridad, incluidas las obligaciones de privacidad y libertades civiles, se entienden y gestionan |  |  |
| *ID.GV-4* | Los procesos de gobernanza y gestión de riesgos abordan los riesgos de ciberseguridad |  |  |
| *ID.RA* | La organización comprende el riesgo de ciberseguridad para las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), activos organizacionales e individuos. |  |  |
| *ID.RA-1* | Las vulnerabilidades de los activos se identifican y documentan |  |  |
| *ID.RA-2* | La inteligencia sobre amenazas cibernéticas se recibe de foros y fuentes de intercambio de información |  |  |
| *ID.RA-3* | Las amenazas, tanto internas como externas, se identifican y documentan. |  |  |
| *ID.RA-4* | Se identifican los posibles impactos en el negocio y las probabilidades |  |  |
| *ID.RA-5* | Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo. |  |  |
| *ID.RA-6* | Las respuestas al riesgo se identifican y priorizan |  |  |
| *ID.RM* | Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y utilizan para respaldar las decisiones de riesgo operativo. |  |  |
| *ID.RM-1* | Los procesos de gestión de riesgos son establecidos, gestionados y acordados por las partes interesadas de la organización |  |  |
| *ID.RM-2* | La tolerancia al riesgo organizacional se determina y se expresa claramente |  |  |
| *ID.RM-3* | La determinación de la organización de la tolerancia al riesgo se basa en su papel en la infraestructura crítica y en el análisis de riesgos específicos del sector. |  |  |
| *ID.SC* | Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro. |  |  |
| *ID.SC-1* | Los procesos de gestión de riesgos de la cadena de suministro cibernética son identificados, establecidos, evaluados, gestionados y acordados por las partes interesadas de la organización. |  |  |
| *ID.SC-2* | Los proveedores y socios externos de los sistemas, componentes y servicios de información se identifican, priorizan y evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético. |  |  |
| *ID.SC-3* | Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de ciberseguridad de una organización y el Plan de gestión de riesgos de la cadena de suministro cibernético. |  |  |
| *ID.SC-4* | Los proveedores y socios externos son evaluados de manera rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluaciones para confirmar que cumplen con sus obligaciones contractuales. |  |  |
| *ID.SC-5* | La planificación y las pruebas de respuesta y recuperación se realizan con proveedores y proveedores externos. |  |  |
| *PR* | Desarrollar e implementar salvaguardas apropiadas para asegurar la entrega de servicios críticos. |  |  |
| *PR.AC* | El acceso a los activos físicos y lógicos y las instalaciones asociadas se limita a usuarios, procesos y dispositivos autorizados, y se gestiona de manera coherente con el riesgo evaluado de acceso no autorizado a actividades y transacciones autorizadas. |  |  |
| *PR.AC-1* | Las identidades y credenciales se emiten, administran, verifican, revocan y auditan para dispositivos, usuarios y procesos autorizados. |  |  |
| *PR.AC-2* | El acceso físico a los activos se gestiona y protege |  |  |
| *PR.AC-3* | Se gestiona el acceso remoto. |  |  |
| *PR.AC-4* | Los permisos y autorizaciones de acceso se gestionan, incorporando los principios de menor privilegio y separación de funciones. |  |  |
| *PR.AC-5* | La integridad de la red está protegida (por ejemplo, segregación de red, segmentación de red) |  |  |
| *PR.AC-6* | Las identidades se prueban y se unen a credenciales y se afirman en interacciones |  |  |
| *PR.AC-7* | Los usuarios, dispositivos y otros activos están autenticados (p. Ej., Factor único, factor múltiple) proporcionales al riesgo de la transacción (p. Ej., Riesgos de seguridad y privacidad de las personas y otros riesgos organizacionales) |  |  |
| *PR.AC-7* | Los usuarios, dispositivos y otros activos están autenticados (p. Ej., Factor único, factor múltiple) proporcionales al riesgo de la transacción (p. Ej., Riesgos de seguridad y privacidad de las personas y otros riesgos organizacionales) |  |  |
| *IMBÉCIL* | El personal y los socios de la organización reciben educación sobre concientización en seguridad cibernética y están capacitados para realizar sus deberes y responsabilidades relacionados con la seguridad cibernética, de conformidad con las políticas, procedimientos y acuerdos relacionados. |  |  |
| *PR.AT-1* | Todos los usuarios están informados y capacitados. |  |  |
| *PR.AT-2* | Los usuarios privilegiados comprenden sus roles y responsabilidades. |  |  |
| *PR.AT-3* | Las partes interesadas de terceros (por ejemplo, proveedores, clientes, socios) entienden sus roles y responsabilidades |  |  |
| *PR.AT-4* | Los altos ejecutivos comprenden sus roles y responsabilidades. |  |  |
| *PR.AT-5* | El personal físico y de ciberseguridad comprende sus roles y responsabilidades. |  |  |
| *PR.DS* | La información y los registros (datos) se administran de acuerdo con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información. |  |  |
| *PR.DS-1* | Los datos en reposo están protegidos |  |  |
| *PR.DS-2* | Los datos en tránsito están protegidos |  |  |
| *PR.DS-3* | Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición. |  |  |
| *PR.DS-4* | Capacidad adecuada para garantizar que se mantenga la disponibilidad |  |  |
| *PR.DS-5* | Se implementan protecciones contra fugas de datos. |  |  |
| *PR.DS-6* | Los mecanismos de verificación de integridad se utilizan para verificar el software, el firmware y la integridad de la información. |  |  |
| *PR.DS-7* | Los entornos de desarrollo y prueba están separados del entorno de producción. |  |  |
| *PR.DS-8* | Los mecanismos de comprobación de integridad se utilizan para verificar la integridad del hardware. |  |  |
| *PR.IP* | Las políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de gestión y la coordinación entre las entidades de la organización), los procesos y los procedimientos se mantienen y utilizan para gestionar la protección de los sistemas y activos de información. |  |  |
| *PR.IP-1* | Se crea y mantiene una configuración básica de los sistemas de tecnología de la información / control industrial que incorpora principios de seguridad (por ejemplo, el concepto de menor funcionalidad) |  |  |
| *PR.IP-2* | Se implementa un ciclo de vida de desarrollo de sistemas para administrar sistemas |  |  |
| *PR.IP-3* | Los procesos de control de cambio de configuración están en su lugar |  |  |
| *PR.IP-4* | Las copias de seguridad de la información se realizan, mantienen y prueban |  |  |
| *PR.IP-5* | Se cumplen las políticas y regulaciones sobre el entorno operativo físico para los activos de la organización. |  |  |
| *PR.IP-6* | Los datos se destruyen de acuerdo con la política. |  |  |
| *PR.IP-7* | Se mejoran los procesos de protección. |  |  |
| *PR.IP-8* | La efectividad de las tecnologías de protección es compartida |  |  |
| *PR.IP-9* | Los planes de respuesta (respuesta a incidentes y continuidad del negocio) y los planes de recuperación (recuperación de incidentes y recuperación de desastres) están implementados y administrados |  |  |
| *PR.IP-10* | Se prueban los planes de respuesta y recuperación |  |  |
| *PR.IP-11* | La ciberseguridad está incluida en las prácticas de recursos humanos (por ejemplo, des aprovisionamiento , selección de personal) |  |  |
| *PR.IP-12* | Se desarrolla e implementa un plan de gestión de vulnerabilidades. |  |  |
| *PR.MA* | El mantenimiento y las reparaciones de los componentes del control industrial y del sistema de información se realizan de acuerdo con las políticas y procedimientos. |  |  |
| *PR.MA-1* | El mantenimiento y la reparación de los activos de la organización se realizan y registran, con herramientas aprobadas y controladas. |  |  |
| *PR.MA-2* | El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de una manera que impide el acceso no autorizado. |  |  |
| *PR.PT* | Las soluciones de seguridad técnica se gestionan para garantizar la seguridad y la resistencia de los sistemas y activos, de acuerdo con las políticas, procedimientos y acuerdos relacionados. |  |  |
| *PR.PT-1* | Los registros de auditoría / registro se determinan, documentan, implementan y revisan de acuerdo con la política |  |  |
| *PR.PT-2* | Los medios extraíbles están protegidos y su uso está restringido de acuerdo con la política. |  |  |
| *PR.PT-3* | El principio de menor funcionalidad se incorpora mediante la configuración de sistemas para proporcionar solo capacidades esenciales |  |  |
| *PR.PT-4* | Las redes de comunicaciones y control están protegidas. |  |  |
| *PR.PT-5* | Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, intercambio en caliente) para lograr los requisitos de resistencia en situaciones normales y adversas |  |  |
| *Delaware* | Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética. |  |  |
| *DE.AE* | Se detecta actividad anómala y se entiende el impacto potencial de los eventos. |  |  |
| *DE.AE-1* | Se establece y administra una línea base de operaciones de red y flujos de datos esperados para usuarios y sistemas. |  |  |
| *DE.AE-2* | Los eventos detectados se analizan para comprender los objetivos y métodos de ataque. |  |  |
| *DE.AE-3* | Los datos de eventos se recopilan y se correlacionan de múltiples fuentes y sensores |  |  |
| *DE.AE-4* | Se determina el impacto de los eventos. |  |  |
| *DE.AE-5* | Se establecen umbrales de alerta de incidentes. |  |  |
| *DE.CM* | El sistema de información y los activos son monitoreados para identificar eventos de seguridad cibernética y verificar la efectividad de las medidas de protección. |  |  |
| *DE.CM-1* | La red se supervisa para detectar posibles eventos de ciberseguridad. |  |  |
| *DE.CM-2* | El entorno físico se controla para detectar posibles eventos de ciberseguridad. |  |  |
| *DE.CM-3* | La actividad del personal se controla para detectar posibles eventos de ciberseguridad. |  |  |
| *DE.CM-4* | Se detecta código malicioso |  |  |
| *DE.CM-5* | Se detecta un código móvil no autorizado |  |  |
| *DE.CM-6* | La actividad del proveedor de servicios externos se supervisa para detectar posibles eventos de ciberseguridad. |  |  |
| *DE.CM-7* | Se realiza monitoreo de personal no autorizado, conexiones, dispositivos y software |  |  |
| *DE.CM-8* | Se realizan exploraciones de vulnerabilidad |  |  |
| *DE.DP* | Los procesos y procedimientos de detección se mantienen y prueban para garantizar el conocimiento de eventos anómalos. |  |  |
| *DE.DP-1* | Los roles y responsabilidades para la detección están bien definidos para garantizar la responsabilidad |  |  |
| *DE.DP-2* | Las actividades de detección cumplen con todos los requisitos aplicables. |  |  |
| *DE.DP-4* | La información de detección de eventos se comunica |  |  |
| *DE.DP-5* | Los procesos de detección se mejoran continuamente. |  |  |
| *RS* | Desarrolle e implemente actividades apropiadas para tomar medidas con respecto a un incidente de seguridad cibernética detectado. |  |  |
| *RS.AN* | El análisis se realiza para garantizar una respuesta efectiva y apoyar las actividades de recuperación. |  |  |
| *RS.AN-1* | Se investigan las notificaciones de los sistemas de detección. |  |  |
| *RS.AN-2* | Se entiende el impacto del incidente. |  |  |
| *RS.AN-3* | Se realizan forenses |  |  |
| *RS.AN-4* | Los incidentes se clasifican de acuerdo con los planes de respuesta. |  |  |
| *RS.AN-5* | Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización de fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad) |  |  |
| *RS.CO* | Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de las agencias de aplicación de la ley). |  |  |
| *RS.CO-1* | El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta. |  |  |
| *RS.CO-2* | Los incidentes se informan de acuerdo con los criterios establecidos. |  |  |
| *RS.CO-3* | La información se comparte de acuerdo con los planes de respuesta. |  |  |
| *RS.CO-4* | La coordinación con las partes interesadas ocurre de acuerdo con los planes de respuesta. |  |  |
| *RS.CO-5* | El intercambio voluntario de información se produce con partes interesadas externas para lograr una mayor conciencia de la situación de ciberseguridad. |  |  |
| *RS.IM* | Las actividades de respuesta organizacional se mejoran al incorporar las lecciones aprendidas de las actividades de detección / respuesta actuales y anteriores. |  |  |
| *RS.IM-1* | Los planes de respuesta incorporan las lecciones aprendidas |  |  |
| *RS.IM-2* | Se actualizan las estrategias de respuesta. |  |  |
| *RS.MI* | Las actividades se realizan para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente. |  |  |
| *RS.MI-1* | Los incidentes están contenidos |  |  |
| *RS.MI-2* | Los incidentes se mitigan |  |  |
| *RS.MI-3* | Las vulnerabilidades recientemente identificadas se mitigan o documentan como riesgos aceptados |  |  |
| *RS.RP* | Los procesos y procedimientos de respuesta se ejecutan y mantienen, para garantizar la respuesta a incidentes de ciberseguridad detectados. |  |  |
| *RS.RP-1* | El plan de respuesta se ejecuta durante o después de un incidente. |  |  |
| *RC* | Desarrolle e implemente actividades apropiadas para mantener planes de resiliencia y restaurar cualquier capacidad o servicio que se haya visto afectado debido a un incidente de ciberseguridad. |  |  |
| *RC.CO* | Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores). |  |  |
| *RC.CO-1* | Se gestionan las relaciones públicas. |  |  |
| *RC.CO-2* | La reputación se repara después de un incidente. |  |  |
| *RC.CO-3* | Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como a los equipos ejecutivos y de gestión. |  |  |
| *RC.IM* | La planificación y los procesos de recuperación se mejoran al incorporar las lecciones aprendidas en actividades futuras. |  |  |
| *RC.IM-1* | Los planes de recuperación incorporan las lecciones aprendidas |  |  |
| *RC.IM-2* | Se actualizan las estrategias de recuperación. |  |  |
| *RC.RP* | Los procesos y procedimientos de recuperación se ejecutan y mantienen para garantizar la restauración de los sistemas o activos afectados por incidentes de ciberseguridad. |  |  |
| *RC.RP-1* | El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad |  |  |

## Principios y prácticas de CIS RAM

CIS RAM adopta los tres principios y diez prácticas del Análisis de Riesgo del Deber de Cuidados. Los tres principios establecen las características de las evaluaciones de riesgos que se alinean con las expectativas regulatorias y legales. Las diez prácticas describen características de las evaluaciones de riesgos que hacen alcanzables los tres principios.

## Principios

1. El análisis de riesgos debe considerar los intereses de todas las partes que puedan verse perjudicadas por el riesgo.

2. Los riesgos deben reducirse a un nivel que las autoridades y las partes potencialmente afectadas consideren apropiadas.

3. Las salvaguardas no deben ser más onerosas que los riesgos contra los que protegen.

## Prácticas

1. El análisis de riesgos considera la probabilidad de que ciertas amenazas puedan crear magnitudes de impacto.

2. Los riesgos y las salvaguardas se evalúan utilizando los mismos criterios para poder compararlos.

3. Los puntajes de impacto y probabilidad tienen un componente cualitativo que expone de manera concisa las preocupaciones de las partes interesadas, las autoridades y la organización evaluadora.

4. Los puntajes de impacto y probabilidad se derivan de un cálculo numérico que permite la comparabilidad entre todos los riesgos, salvaguardas y criterios de aceptación de riesgos evaluados.

5. Las definiciones de impacto aseguran que la magnitud del daño a una parte se equipare con la magnitud del daño a otras.

6. Las definiciones de impacto deben tener un límite explícito entre aquellas magnitudes que serían aceptables para todas las partes y aquellas que no lo serían.

7. Dirección de definiciones de impacto; La misión o la utilidad de la organización para explicar por qué la organización y otros involucran riesgos, los objetivos egoístas de la organización y las obligaciones de la organización de proteger a los demás del daño.

8. El análisis de riesgos se basa en un estándar de atención para analizar los controles actuales y las garantías recomendadas.

9. El riesgo es analizado por expertos en la materia que usan evidencia para evaluar riesgos y salvaguardas.

10. Las evaluaciones de riesgos no pueden evaluar todos los riesgos previsibles. Las evaluaciones de riesgos vuelven a ocurrir para identificar y abordar más riesgos con el tiempo.

## Pasos para la evaluación de riesgos

Durante el Paso 1 (Definición del alcance y las sesiones de programación), la organización determinará qué activos de información incluir en su evaluación. También identificarán a los dueños de negocios y administradores técnicos que proporcionarán evidencia y entrevistas para evaluar esos activos. El evaluador de riesgos luego programará sesiones de entrevistas con esos propietarios y delegados.

En el Paso 2 (Definición de criterios de evaluación de riesgos), la organización definirá las reglas mediante las cuales evaluarán y puntuará los riesgos. Definirán su misión (el valor que aportan a los demás) y sus obligaciones (el potencial de daño contra los demás) para establecer lo que están tratando de proteger. Luego definirán los esquemas de puntuación que se utilizarán para el impacto y la estimación de probabilidad.

En el Paso 3 (Definición de los criterios de aceptación de riesgos), la organización establecerá su tolerancia al riesgo seleccionando una combinación de la probabilidad de un impacto que sería tolerable para todas las partes (la organización y las partes que pueden verse perjudicadas por los riesgos realizados).

En el Paso 4 (Evaluación de Riesgos - basado en el control) evaluador de riesgos evaluará los riesgos de los activos de información. Para las organizaciones de nivel 1, el análisis incluye las siguientes actividades:

• “Recopilar evidencia” implica una revisión de documentos, como políticas, procedimientos, estándares y puntos de referencia. También incluye entrevistas con la gerencia y el personal. La recopilación de evidencia también implica la observación de configuraciones, artefactos, instalaciones, registros y procesos de trabajo para determinar si operan de manera segura o vulnerable.

Las organizaciones de nivel 1 también deberían considerar revisar las configuraciones de los controles y buscar evidencia de su efectividad. Esto puede ser un desafío para las organizaciones a este nivel. Los escáneres de vulnerabilidades y los escáneres de configuración que utilizan políticas SCAP pueden proporcionar un análisis eficiente de los sistemas técnicos para ayudar en este análisis.

• “Modelar las amenazas” implica la mayor variedad de enfoques que dependen de la madurez de ciberseguridad de la organización. Sin embargo, cada organización modelará los riesgos con al menos estos componentes: teniendo en cuenta los controles CIS que deberían existir para proteger los activos de información; determinar si esas salvaguardas están efectivamente establecidas para proteger los activos de información; identificar vulnerabilidades que pueden permitir violaciones de los activos; e identificar amenazas que podrían aprovechar esas vulnerabilidades.

• Durante la “Evaluación de riesgos”, la organización estimará la probabilidad y el impacto de los riesgos. Las estimaciones se basarán en la puntuación y los criterios establecidos en el Paso 2. La puntuación de riesgo se calculará automáticamente para determinar si las implementaciones actuales de los Controles CIS ya son razonables.

Durante el Paso 5 (Proponer salvaguardas), la organización considerará cómo abordar los riesgos irrazonables seleccionando los Controles CIS que deben implementarse para abordar cada riesgo, y específicamente cómo se implementarán los controles. Estas salvaguardas pueden incluir dispositivos de seguridad, salvaguardas físicas, capacitación, procesos de supervisión u otros métodos. Luego, el evaluador de riesgos probará la razonabilidad de las salvaguardas durante “Evaluar las salvaguardas propuestas”. El evaluador de riesgos evaluará las salvaguardas propuestas utilizando los mismos criterios que se usaron para evaluar los riesgos.

Una plantilla de plan de proyecto está disponible en el documento complementario CIS\_RAM\_Workbook.

## Manual de análisis de riesgos, una introducción

Las leyes, regulaciones y estándares de seguridad de la información no esperan que el público pueda o prevenga todos los incidentes de seguridad de la información. En su lugar, nos hacen responsables de mirar hacia adelante en lo que podría salir mal y de utilizar salvaguardas que no sean demasiado pesadas para evitar ese daño. Esa es la esencia del análisis de riesgos del deber de cuidado en el que se basa la RAM CIS.

## Bases en Derecho y Regulación

El método de análisis de riesgos de CIS RAM fue diseñado para proporcionar un terreno común para especialistas en seguridad y gerentes de negocios, y para autoridades legales y reguladoras que deben evaluar la suficiencia de las salvaguardas de seguridad.

En Ecuador en abril del 2002 debido a la creciente aparición del internet y la necesidad de globalización se creó el primer intento de normalización de las comunicaciones, esto es importante ya que hoy por hoy es la principal herramienta de comunicaciones entre pares y empresas y también esto representa según la normativa un bien digital que se debe proteger y garantizar a la par que el manejo de comunicaciones digitales ha causado el interés de atacantes sobre estos activos digitales.

Los organismos nacionales e internacionales de normas de seguridad de la información desarrollaron métodos de evaluación de riesgos, como las publicaciones especiales NIST 800-30, ISO 27005 y RISK IT para ayudar al público a evaluar los riesgos en entornos de tecnología de la información. Estas normas de seguridad de la información también utilizaron la misma ecuación utilizada por los reguladores de los EE. UU. - "Riesgo = Impacto x Probabilidad" - para expresar la previsibilidad de los daños que podrían sufrir los sistemas de información e información.

Tabla 5: Alineación de principios y prácticas de RAM de CIS a la ley, regulaciones y estándares de seguridad - Anexo 3.2.

|  |  |  |  |
| --- | --- | --- | --- |
| **Principios y prácticas de CIS RAM y DoCRA** | **Ley** | **Reglamento** | **Normas de seguridad** |
| El análisis de riesgos debe considerar los intereses de todas las partes que puedan verse perjudicados por el riesgo. |  |  |  |
| Los riesgos deben reducirse a un nivel que las autoridades y las partes potencialmente afectadas consideren apropiadas. |  |  |  |
| Las salvaguardas no deben ser más onerosas que los riesgos contra los que protegen. |  |  |  |
| El análisis de riesgos considera la probabilidad de que ciertas amenazas puedan crear magnitudes de impacto. |  |  |  |
| Los riesgos y las salvaguardas se evalúan utilizando los mismos criterios para poder compararlos. |  |  |  |
| Los puntajes de impacto y probabilidad tienen un componente cualitativo que expone de manera concisa las preocupaciones de las partes interesadas, las autoridades y la organización evaluadora. |  |  |  |
| Los puntajes de impacto y probabilidad se derivan de un cálculo numérico que permite la comparabilidad entre todos los riesgos, salvaguardas y criterios de aceptación de riesgos evaluados. |  |  |  |
| Las definiciones de impacto aseguran que la magnitud del daño a una de las partes se equipare con la magnitud del daño a los demás. |  |  |  |
| Las definiciones de impacto deben tener un límite explícito entre aquellas magnitudes que serían aceptables para todas las partes y aquellas que no lo serían. |  |  |  |
| Dirección de definiciones de impacto; La misión o la utilidad de la organización para explicar por qué la organización y otros involucran el riesgo, los objetivos egoístas de la organización y las obligaciones de la organización de proteger a otros del daño. |  |  |  |
| El análisis de riesgos se basa en un estándar de atención para analizar los controles actuales y las garantías recomendadas. |  |  |  |
| El riesgo es analizado por expertos en la materia que usan evidencia para evaluar riesgos y salvaguardas. |  |  |  |
| Las evaluaciones de riesgos no pueden evaluar todos los riesgos previsibles. Las evaluaciones de riesgos vuelven a ocurrir para identificar y abordar más riesgos con el tiempo. |  |  |  |

Las organizaciones que realizan evaluaciones de riesgos utilizando el CIS RAM tendrán un plan para implantar los Controles CIS V7 que sea razonable y defendible tanto para las autoridades como para los expertos.

## ¿Vale la pena este análisis extendido? En pocas palabras, sí.

Los controles de seguridad de la información a menudo se consideran un obstáculo para los negocios. Los usuarios a menudo se quejan de que los controles de seguridad obstaculizan la productividad, la eficiencia, la facilidad de colaboración y comunicación, y otras preocupaciones que afectan el negocio. Las organizaciones deben tomar estas quejas en serio. Afortunadamente, los reguladores han proporcionado a las organizaciones un medio para evaluar estas preocupaciones. Además, los tribunales consideran la carga de las salvaguardas en los juicios y entenderían el razonamiento que proporciona este análisis de riesgos.

Al evaluar los riesgos y sus salvaguardas recomendadas utilizando el mismo criterio, las organizaciones aseguran que el análisis de riesgos aborde las preocupaciones de todas las partes dentro y fuera de su organización, y proporcione evidencia de su decisión consciente a los reguladores y jueces.

## Tipo de estudio

### Nivel de evaluación de riesgos

Los Niveles indican "cómo una organización ve el riesgo de ciberseguridad y los procesos establecidos para gestionar ese riesgo". Los Niveles se definen por NIST de la siguiente manera.

**Nivel 1: Parcial**

* Proceso de gestión de riesgos: informal y ad hoc.
* Programa integrado de gestión de riesgos: conciencia limitada dentro de la organización.
* Participación externa: no se coordina con entidades externas.

**Nivel 2: Riesgo informado**

* Proceso de gestión de riesgos: informado por los objetivos de riesgo de la organización.
* Programa integrado de gestión de riesgos: procesos y procedimientos informados por el riesgo y aprobados por la administración.
* Participación externa: no se coordina con entidades externas.

**Nivel 3: Repetible**

* Proceso de gestión de riesgos: aplicado a través de políticas y actualizado con cambios en el entorno y las amenazas.
* Programa integrado de gestión de riesgos: las políticas y procesos informados sobre riesgos se utilizan en toda la empresa. El personal está capacitado e informado para trabajar de manera segura.
* Participación externa: recibir información de los socios para tomar decisiones internas basadas en el riesgo.

**Nivel 4: Adaptativo**

* Proceso de gestión de riesgos: adaptable a través de las lecciones aprendidas y la mejora continua.
* Programa integrado de gestión de riesgos: cultura de conciencia de seguridad en toda la empresa y mejora continua basada en lecciones aprendidas e información externa.
* Participación externa: compartir información de seguridad y amenazas con los socios.

### Elección de una perspectiva de ciberseguridad

En base a los niveles del NIST y los requerimientos de implementación recogidos en las encuestas realizadas y con el alcance estipulado en el acuerdo de implementación se observa que el nivel de seguridad más adecuado es el nivel 1.

Nivel NIST: organizaciones de Nivel 1. Los materiales de Nivel 1 son los más adecuados para organizaciones que no coordinan sus planes y requisitos de seguridad de la información en toda la organización. La seguridad de la información está impulsada en gran medida por la gestión de la tecnología.

Experiencia: la organización puede identificar amenazas genéricas, pero no métodos específicos para piratear sistemas, dispositivos y aplicaciones.

Tiempo: la organización puede absorber el tiempo necesario para evaluar los riesgos de la información a nivel de sistemas, dispositivos y aplicaciones genéricos.

## Definiendo el Alcance físico

Las organizaciones deben realizar evaluaciones de riesgos en relación con un alcance claramente definido de los activos de información. Por lo general, el nombre limita el alcance de los activos, como “activos de información que contienen información confidencial”, “el centro de datos”, “áreas de práctica de ingeniería y tecnologías que los respaldan” o una división comercial específica.

Si bien es posible seleccionar activos de información no relacionados para una evaluación, o un subconjunto de activos dentro de un alcance más amplio, la organización que recibe la evaluación y está haciendo inversiones y decisiones de priorización basadas en sus hallazgos se sentirá más cómoda cuando los activos de información están asociados con una entidad comercial o un proceso comercial. De lo contrario, los resultados de la evaluación de riesgos pueden parecer dispersos y no relacionados.

Del mismo modo, al evaluar el riesgo de un conjunto de activos de información, tiene sentido considerar un conjunto de activos que pueden afectar directamente la seguridad de los demás. Por ejemplo, una evaluación de riesgos que examina un conjunto de aplicaciones también debe incluir los dispositivos de red que conectan las aplicaciones a otros activos y otras redes, así como los procesos que se utilizan para desarrollar y administrar esas aplicaciones. Estos sistemas están directamente conectados entre sí y dependen unos de otros, por lo que sus riesgos se asocian fácilmente entre sí.

Las organizaciones no pueden examinar todos los activos de información de manera exhaustiva en una única evaluación de riesgos, por lo que su alcance debe considerar el tiempo y los recursos disponibles para la evaluación.

Tabla 7: Alcance de activos de empresa.

|  |  |  |  |
| --- | --- | --- | --- |
| Tipo de activo | Clase de Activo | Área de negocio | Custodio |
| Información | Documentos | Contabilidad | Contabilidad |
| Servidores | Server | Help Desk | Help Desk |
| Equipos de red | Equipos de red | Help Desk | Help Desk |
| Equipo | Equipos | Márquetin | Carrito online |
|  |  |  |  |

## Programación de sesiones de entrevista

Las sesiones de entrevista serán de actualidad y deben abordar un tema o temas estrechamente relacionados para cada conversación. Las sesiones de entrevista pueden centrarse en los controles de CIS o en los activos de información y las clases de activos.

Por ejemplo, las sesiones de entrevistas que se centran en los Controles CIS reunirían al personal y la gerencia que saben cómo se implementa y opera cada control. Una sesión puede ser dedicado a CIS Control 1 para comprender cómo se inventarían los dispositivos. Se puede programar otro para discutir CIS Control 2 para comprender qué salvaguardas existen para el software de inventario. O, si el mismo personal conoce ambas salvaguardas, la n quizás una sesión podría combinar ambos temas.

Del mismo modo, si los evaluadores de riesgos programan sesiones en torno a activos de información o clases de activos, entonces sería apropiado incluir propietarios de negocios y propietarios técnicos de esos sistemas para comprender cómo se aplican los Controles CIS asociados a cada activo o clase de activo.

## Programación de revisiones de evidencia

Los evaluadores de riesgos utilizan sesiones de revisión de evidencia para examinar los activos de información y; determine si se ajustan a los Controles CIS y evalúe si serían eficaces contra las amenazas previsibles.

Las sesiones de revisión de evidencia deben programarse después de las entrevistas para que los evaluadores de riesgos comprendan el panorama general del entorno de seguridad antes de tratar de entender por qué ciertos conjuntos están configurados de la manera en que están.

Se propone la siguiente tabla para manejar los avances del proyecto:

Tabla 8: Plan de proyecto para implementación.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Paso | Tarea | Roles Claves | Duración | Asignado a | Fecha de inicio | Fecha de finalización | Status |
| 1 | Definición del alcance y la programación de sesiones | Ejecutivos, Gerencia, Asesor | 1 día |  |  |  |  |
| 2 | Definición de criterios de evaluación de riesgos | Gerente, Asesor | 2 horas |  |  |  |  |
| 3 | Definición de criterios de aceptación de riesgos | Ejecutivos, Gerencia, Asesor | 2 horas |  |  |  |  |
| 4 | Evaluación de riesgos (basada en control) |  | Ámbito dependiente |  |  |  |  |
| 4.1 | Reunir evidencias | Personal, Gerencia, Asesor |  |  |  |  |  |
| 4.2 | Modelar las amenazas | Personal, Gerencia, Asesor |  |  |  |  |  |
| 4.3 | Evaluación de riesgo | Asesor |  |  |  |  |  |
| 5 | Proponer salvaguardas |  | Ámbito dependiente |  |  |  |  |
| 5.1 | Evaluar las salvaguardas propuestas | Asesor, Gerencia |  |  |  |  |  |
| 6 | Aplicación de controles propuestos | Asesor. |  |  |  |  |  |