  
**FACULTAD DE ARQUITECTURA E INGENIERIA  
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   
MAESTRIA EN CIBERSEGURIDAD

QUITO, septiembre 2019

Nota del autor

[Incluya información sobre becas o ayudas y una dirección postal completa.]

Resumen

El riesgo, el tema del capítulo anterior, es el enfoque más conocido y quizás el mejor estudiado dentro de una clase mucho más amplia de evaluaciones de seguridad cibernética. Sin embargo, la evaluación de riesgos no es el único enfoque posible para la seguridad cibernética. Existen otros enfoques y métricas como la resiliencia y podrían ser potencialmente muy valiosos para los defensores de los sistemas ICS.

[El resumen ha de tener una longitud de un párrafo de entre 150 y 250 palabras. sin sangría. Los títulos de sección, como la palabra Resumen anterior, no se consideran títulos, por lo que no se usa formato de título en negrita. En su lugar, use el estilo Título de sección. Este estilo inicia automáticamente la sección en una nueva página, por lo que no es necesario que agregue saltos de página. Tenga en cuenta que todos los estilos de esta plantilla están disponibles en la pestaña Inicio de la cinta, en la galería de estilos.]

Palabras clave: [Haga clic aquí para agregar palabras clave.]

Implementación de controles CIS en la Empresa Tatoo Adventure Gear.

# El Problema de investigación

## Planteamiento del problema

### Diagnostico.

Tatoo Adventure Gear ha crecido durante el último año incorporando a sus servicios dos nuevas innovaciones de negocios, uno es el mejoramiento de su sitio web representado por la optimización de su sistema 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 3 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 no cuenta con políticas de seguridad de la información, sin embargo, el área de desarrollo web, el área de desarrollo de ERP y Helpdesk 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.

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.

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 debemos 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 cuenta con 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 cuenta con 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.

### Pronostico.

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 podemos observar la cantidad de ventas y de usuarios ha tenido un crecimiento importante para la empresa, de la mano de este crecimiento los equipos y software también han aumentado, 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 políticas de seguridad a la medida, estas políticas tienen como objetivo evitar en lo posible daños, la pérdida de reputación de la empresa, pérdidas económicas y afectación de productividad.

### Control de pronostico

Se necesita colocar un grupo 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.

Además 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 vamos a denominar como riesgo razonable, el cual generara un plan de “seguridad razonable”.

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, pérdida de reputación de la empresa, pérdidas económicas y afectación de productividad.

## Objetivos

### Objetivo general

Implementar controles de ciberseguridad en la empresa Tatoo Adventure Gear en las oficinas de Ecuador mediante la aplicación de las seis primeras acciones fundamentales sugeridas por el CENTER FOR INTERNET SECURITY para resguardar y proteger 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 y políticas de ciberseguridad.
* Determinar los controles de seguridad que se aplicaran a Tatoo Adventure Gear sede Ecuador mediante el análisis de los indicadores de la CIS-RAM que permitan la mitigación de las vulnerabilidades encontradas mediante los controles CIS asignados.
* 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 metodológica}

### 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, 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.

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.

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 La Favorita que se divulgo en abril del 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.

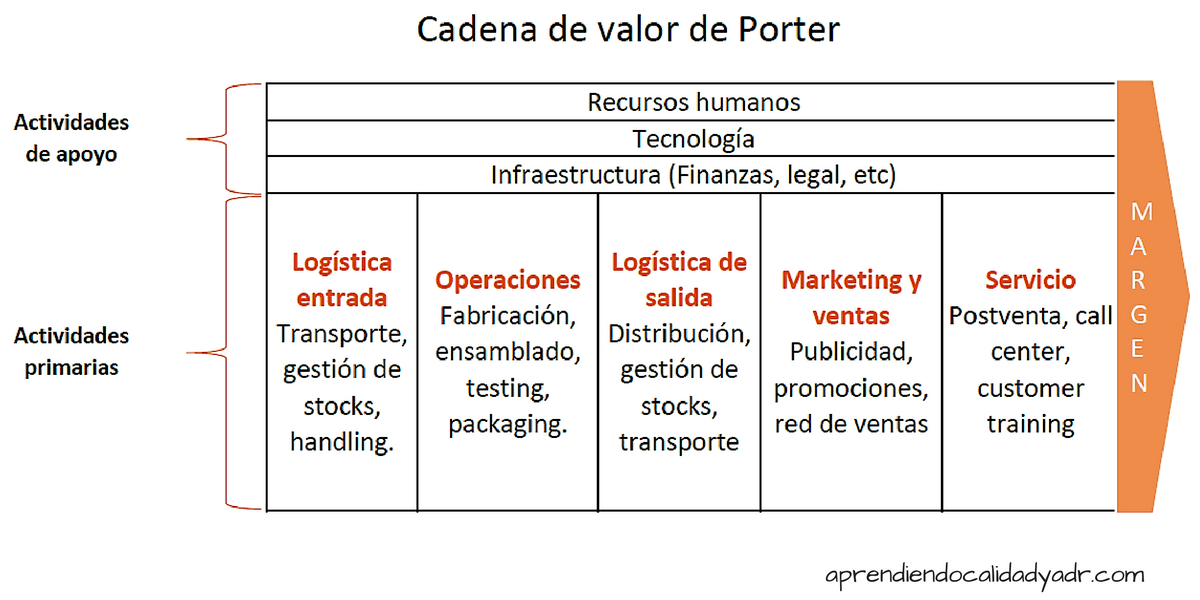


Figure 1: Estructura de la cadenas de valor de la empresa modelo de Retail, como se puede ver el area de tecnologia es parte de toda la cadenay por lo tanto aporta en casi tidas las areas de la empresa.

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, podemos 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.

Para organizar nuestro esfuerzo, se requiere un Framework. Un Framework se presta a muchas metáforas fácilmente relacionadas. Necesitamos un Framework para nuestro programa de seguridad de la información, ahora vamos a segmentar nuestro programa de seguridad de la información en unidades lógicas y tangibles que llamaremos dominios. Los dominios de seguridad están asociados con agrupaciones designadas de actividades, sistemas o recursos relacionados.

### 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. Vamos 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 estamos tratando de lograr y por qué. Comencemos por lo tanto discutiendo los tres principios básicos de la seguridad de la información. Luego observamos la creciente amenaza global, que incluye quién está detrás de los ataques, su motivación y cómo atacan. Aplicamos este conocimiento para construir el marco de nuestro programa de seguridad de la información y cómo redactamos nuestras políticas.

### 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 nos esforzamos por 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 nos viene a la cabeza 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, web masters e ingenieros de redes (Terán, 2014).

### Marco de seguridad cibernética del NIST

Antes de discutir el Marco de seguridad cibernética del NIST en detalle, definamos 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, big data y sistemas físicos. Estos esfuerzos y orientación se centran en los objetivos de seguridad de confidencialidad, integridad y disponibilidad (CIA).

### ¿Cuál es la función del NIST?

Fundada en 1901, NIST es una agencia federal no reguladora 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. 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.

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 Norteamerica. 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.

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, implementar 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.

Referencias

Apellidos, n. s. (Año). Título del artículo. *Título del diario*, Páginas desde - hasta.

Apellidos, n. s. (Año). *Título del libro.* Nombre de la ciudad: Nombre del editor.

Notas al pie

1[Agregue notas al pie, si corresponde, en su propia página después de las referencias. Para los requisitos de formato de APA, simplemente escriba sus propias referencias y notas al pie. Para dar formato a una referencia de nota al pie, seleccione el número y, después, en la Galería de estilos de la pestaña Inicio, haga clic en Referencia de nota al pie. En el cuerpo de una nota al pie, como en este ejemplo,se usa el estilo de texto Normal. (Nota: Si elimina esta nota al pie de ejemplo, no se olvide de eliminartambién su referencia en el texto. Está al final del párrafo Título 2 de ejemplo de la primera página del contenido del cuerpo de esta plantilla).]

Tablas

Tabla 1

[Título de tabla]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Encabezado de columna | Encabezado de columna | Encabezado de columna | Encabezado de columna | Encabezado de columna |
| Encabezado de fila | 123 | 123 | 123 | 123 |
| Encabezado de fila | 456 | 456 | 456 | 456 |
| Encabezado de fila | 789 | 789 | 789 | 789 |
| Encabezado de fila | 123 | 123 | 123 | 123 |
| Encabezado de fila | 456 | 456 | 456 | 456 |
| Encabezado de fila | 789 | 789 | 789 | 789 |

Nota: [Coloque todas las tablas del artículo en una sección de tablas, después de las referencias (y, si corresponde, de las notas al pie). Use una página nueva para cada tabla e incluya un número de tabla y un título de tablapara cada una, como se muestra en esta página. Todo el texto explicativo aparece en una nota de tabla después de la tabla, como en esta. Use el estilo de tabla o ilustración, disponible en la galería de estilos de la pestaña Inicio, para agregar el espaciado entre la tabla y la nota Las tablas en el formato de APA pueden usar un interlineado de una línea o de 1,5 líneas. Incluya un título para cada fila o columna, incluso si el contenido parece obvio. Se configuró un estilo de tabla predeterminado para esta plantilla que cumple con las normas del estilo APA. Para insertar una tabla, en la pestaña Insertar, haga clic en Tabla.]

Título de ilustraciones

Ilustración 1. [Incluya todas las ilustraciones en su propia sección, después de las referencias (y, si corresponde, de las notas al pie y las tablas). Incluya un título numerado para cada ilustración. Use el estilo de tabla o ilustración para agregar fácilmente espaciado entre la ilustración y el título.]

Para obtener más información sobre todos los elementos del formato de estilo APA, vea el Manual de estilo de la APA, 6.ª edición.

# 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 |  |  |