TRABAJO FINAL DE GRADUACIÓN

DESARROLLO DE UNA PROPUESTA PARA LA IMPLEMENTACIÓN DE PROTOCOLOS BASADOS EN EL MARCO COBIT 2019 PARA LA GESTIÓN DEL DEPARTAMENTO DE TI DE LA EMPRESA SITEC S.A. (SISTEMAS INTEGRADOS DE SEGURIDAD S.A)

PARA LA OBTENCIÓN DEL GRADO DE BACHILLERATO EN INGENIERÍA INFORMÁTICA

Sustentante:

Roberto Valverde Quesada

FEBRERO 2025

Índice

Tabla de tablas

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Antecedentes Y Justificación Del Proyecto

1.1.1 Antecedentes Del Contexto De La Empresa

Nombre de la empresa: SITEC Sistemas Integrados de Seguridad S.A.

Año de fundación: SITEC Seguridad se funda en el año 2010

Estrategia:

SITEC Seguridad somos una empresa diferente preocupada por la seguridad de nuestros clientes, nos esforzamos día a día por brindar lo mejor en servicio, calor humano y tecnología, contamos con más de 14 años de experiencia en el mercado, enfocados en solucionar las necesidades en seguridad electrónica a nivel nacional.

Creemos en los valores, en la filosofía de la honestidad, el esfuerzo y el profesionalismo, con el fin de reflejar la esencia de SITEC Seguridad en cada uno de nuestros proyectos.

Parte de esa misma filosofía es el interés de formar excelentes profesionales en las áreas que trabajamos. Por ende, nuestros equipos técnicos se capacitan y certifican constantemente en las últimas tendencias, productos y tecnologías de seguridad electrónica y nuestros departamentos de ventas, marketing y desarrollo de proyectos. (SitecSeguridad, 2010)

Visión:

Ser la empresa innovadora en servicios y productos de seguridad electrónica a nivel nacional e internacional con un alto enfoque de servicio al cliente, bajo un valor de mejoramiento continuo y servicio al cliente. (SitecSeguridad, 2010)

Misión:

Brindar a nuestros clientes seguridad a su patrimonio y tranquilidad en sus vidas mediante lo último en sistemas tecnológicos de seguridad, con un personal altamente calificado, con altos valores éticos y morales. (SitecSeguridad, 2010)

Objetivos:

Brindar a nuestros clientes respaldo, confianza y compromiso, con un eficiente servicio e implementación de lo último en tecnología en Seguridad.

Valores:

- Formalidad
- Estructura
- Disciplina
- Control
- Orden
- Mejoramiento continuo
- Trabajo en equipo
- Planificación
- Comunicación

Organización:

La empresa SITEC Seguridad se encuentra organizada básicamente en 3 departamentos generales como los son el área administrativa, el área de ventas y el área técnica.

La empresa Sitec se dedica a la venta e instalación de sistemas electrónicos de seguridad, como sistemas de detección de incendio, controles de acceso, alarmas, cámaras de seguridad entre otros.

Historia:

Nace en 2010 bajo la necesidad de una persona que pasaba por una etapa difícil a nivel laboral que le generaba incertidumbre de su futuro, esta necesidad la plantearon 3 personas que tras varias reuniones forman la empresa y con ella su fundación, empieza con un capital cero y se abre camino en el mercado compitiendo con grandes empresas ya posesionadas en el país hasta llegar a un punto de crecimiento donde decide seguir siendo una empresa grande entre las más pequeñas o la más pequeña.

Tendencia del mercado:

La línea de investigación es una tendencia aplicada a las compañías que manejan sus servicios basados en redes con accesos a internet, donde maneja la información básica de la empresa para su operativa y controles entre sus diferentes bases de datos e información, y también información sensible de clientes, sistemas de facturación, entre otros. Todo lo anterior

hace que las empresas hoy en día se alienen a ciertos procedimientos que garanticen la operativa y lo más importante cuidar los datos e información de sus clientes, esto se conoce como el nuevo oro, en una era donde la información lo es todo y una empresa que pierda esta información puede desaparecer del día a la noche.

1.1.2 Justificación Del Proyecto

La empresa Sistemas Integrados de Seguridad S.A, a la que se referirá a partir de este momento por su nombre comercial SITEC Seguridad, no posee desde su fundación, un departamento que se encargue de la infraestructura de red y del manejo de la información, con lo cual pone en riesgo la continuidad del servicio ante un eventual ataque externo o interno, la falta de un desarrollo en esta área no ha permitido identificar, gestionar, minimizar y controlar los riesgos existentes a nivel interno y externo de la compañía, alguna de las razones del porque SITEC Seguridad debe realizar este proyecto son:

- Decisión de la empresa de realizarlo.
- Un cumplimiento legal al cual debe someterse la empresa.
- Una oportunidad de mejorar el negocio, garantizando la continuidad del negocio por medio de acceso a la información básica de la empresa
- Crecimiento de la empresa y apertura de nuevas sucursales en otros países.

Cabe resaltar que la justificación está fundamentada en el actualmente SITEC Seguridad no dispone de una metodología o estructura en cual apoyarse para la gestión de riesgos relacionados

a los sistemas informáticos y sus diferentes aristas (instalaciones físicas, infraestructura lógica y hardware), lo cual limita considerablemente la capacidad de ofrecer, garantizar y cumplir con buenas prácticas para el manejo de la información.

Por motivos de certificaciones y cumplimientos las empresas deben de asegurar buenas prácticas y entre ellas existe COBIT, utilizaremos específicamente la versión 2019 (última versión) como referencia para implementación de buenas prácticas, esto también se menciona en el acuerdo SUGEF-14-17 (Superintendencia General de Entidades Financieras), el cual exige la implementación de un marco para la gobernanza y gestión, la cual se estructura en 34 procesos para la tecnología de la información.

Otra situación de SITEC Seguridad, es que no posee ningún manual de procedimiento para la gestión de riesgos; al no tener un enfoque claro para este manejo de los datos es donde COBIT puede ser una herramienta muy valiosa para la implementación, optimización y manejo de los riegos, sin dejar de lado que existen también riesgos que podrían impactar negativamente a las empresas a las cuales se les brinda servicios.

Al SITEC Seguridad no contar con una metodología estructurada para la gestión de riegos de TI, se ve reflejado en mayor costo operativo, ya que con cada proyecto requiere de adaptar prácticas a necesidades o solicitudes específicas de sus clientes, así como el manejo de sus datos.

En este caso, es de clara importancia el proyecto para la empresa SITEC Seguridad, en una era donde la tecnología nos une, pero con ella las empresas se exponen a sufrir ataques informáticos de una u otra manera, actualmente la empresa es proveedora de servicios a nivel de

gobierno de Costa Rica y con ello surgen nuevas necesidades planteadas por sus contratantes como lo son:

Trato de la información sensible de sus clientes, almacenamiento de llamadas, correos electrónicos y de contraseñas entre otros; con esto SITEC Seguridad está en un punto en el cual puede continuar tomando oportunidades de negocio o desafortunadamente perdiendo estas, porque se ha demostrado que la tendencia actual de protección y manejo de la información le permite participar de esa rama del negocio con lo cual genera ganancias a las empresas y se reafirma su posicionamiento en el mercado, pero si no es parte de una cultura de seguridad y protección de datos, dejará de ser atractiva para sus clientes actuales y los potenciales.

1.2 Definición Del Problema

La empresa SITEC Seguridad se enfrenta actualmente a uno de los desafíos críticos de cualquier empresa, nos referimos al manejo de los datos, almacenamiento, acceso y aseguramiento de los mismo. A diferencia de muchas organizaciones actuales del mercado, SITEC Seguridad no cuenta con un departamento de Tecnología de la Información (TI) que este dedicado para supervisar y gestionar sus necesidades tecnológicas; además, carece de un responsable específico para esta gestión, lo que nos plantea varias preocupaciones, tomado en consideración en un mundo donde la conectividad y la comunicación son fundamentales para el manejo de la información.

La falta de un equipo interno de TI, además la ausencia de una empresa que brinde ese servicio como outsourcing tecnológico, así como el manejo adecuado de los datos, son algunos de los factores que preocupan actualmente a la empresa. En el escenario actual no existen procedimientos y buenas prácticas para gestionar la información, esenciales para garantizar una comunicación efectiva entre los diferentes departamentos de la compañía. Tomando en consideración que la comunicación y la colaboración entre estos son necesarios y fundamentales para un desarrollo eficiente en SITEC Seguridad y en cualquier otra empresa asociada a esta, y la carencia de esta estructura, así como la falta de control, pone en riesgo la operatividad de la empresa.

Además, la falta de control adecuado para gestionar el flujo de datos de la compañía y el acceso a la información implica un motivo de preocupación adicional en Sitec Seguridad, considerando un entorno empresarial donde hoy en día la información es el activo valioso, la ausencia de un sistema óptimo, actualizado, controlado que pueda garantizar la continuidad del servicio y la protección de los datos internos propios y de los clientes puede tener consecuencias graves para la compañía.

Se debe recalcar que la seguridad de los datos y la disponibilidad de estos son cruciales e indispensables en un mundo donde los datos son considerados el “nuevo petróleo”. La inversión en una infraestructura de TI sólida se ha vuelto indispensable en SITEC Seguridad y actualmente se encuentra en un momento crucial para su desarrollo, donde la implementación de un departamento de TI o la posibilidad de tercerizar estos servicios para satisfacer sus necesidades tecnológicas. Estas alternativas se presentan como pasos esenciales para asegurar su competitividad y su capacidad para proteger los intereses internos y los de sus clientes.

En última instancia, la inversión en tecnología y seguridad de la información es una vital para brindar continuidad y asegurar el éxito a largo plazo de la empresa, donde se busca controlar quien tiene acceso a la información según su rol dentro de la compañía, así como controlar quien puede modificar, crear o eliminar los datos sensibles de la compañía, garantizando la continuidad del negocio por flujo de información.

1.2.1 Problemática

La empresa SITEC Seguridad carece de un área de Tecnologías de la Información (TI) debidamente establecida, esta carencia de una estructura de TI dificulta la obtención de información precisa sobre cómo está configurada la infraestructura tecnología de la compañía, así del cómo se gestiona el flujo de información dentro de la empresa, en consecuencia, se carece de un conocimiento adecuado de los posibles riesgos que puedan existir en la empresa en relación con su datos y manejo de la información.

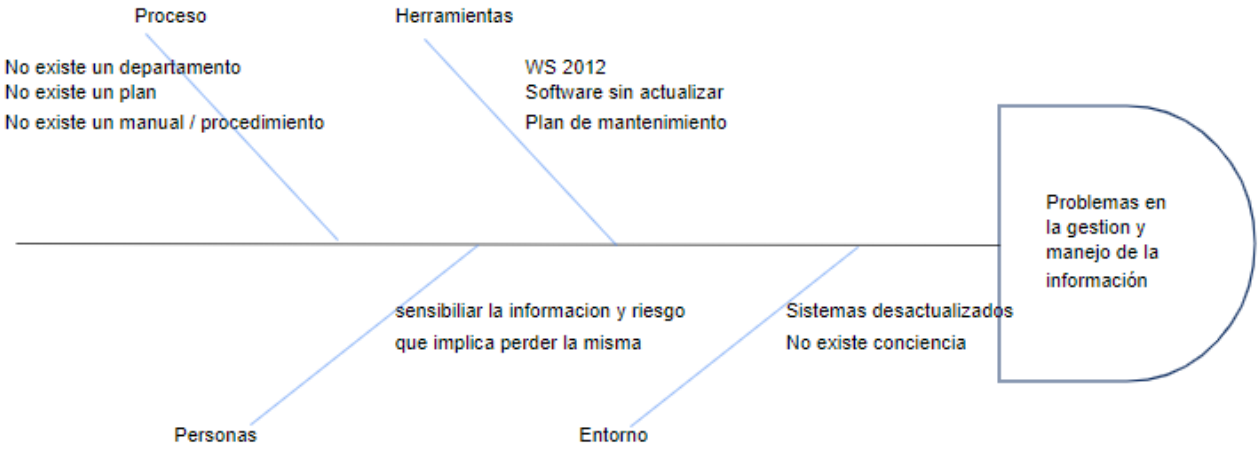
La falta de información representará un desafío significativo para la investigación, lo cual impide tener información previa sobre la cual basar acciones o estrategias relacionadas con la tecnología de la información, así como el poder realizar un levantamiento inicial de reconocimiento de la situación, partiendo de la premisa de que no existe una base previa para apoyarse.

Otro aspecto importante y desafío va ser la involucración de las gerencias de los distintos departamentos y colaboradores en general donde tendrán un papel importante para poder lograr

cumplir los objetivos establecidos de la compañía utilizando un marco de referencia como lo es COBIT 2019.

Diagrama Causa – Efecto

Figura 1
Esquema de un Diagrama Causa – Efecto (Sitec Seguridad, 2024)



El proyecto tiene por solucionar:

1- La propuesta para la creación de una metodología estandarizada para la gestión de riesgos de TI basada en COBIT 2019, que pueda adaptarse a la empresa y en una segunda fase a los clientes de SITEC Seguridad cubriendo las necesidades y requisitos del entorno tecnológico actual.

2- El desarrollo de una metodología integral y efectiva para la gestión de riesgos de la TI, que aborde todos los riesgos asociados, incluyendo los de seguridad y continuidad.

Actualmente, no existe una metodología o herramienta que cubra todos los tipos de riesgos relacionados con la tecnología de la información en SITEC Seguridad.

3- La metodología propuesta en este trabajo fomenta la concienciación en los niveles gerenciales de SITEC Seguridad sobre la importancia de la gestión de riesgos de TI. Esto permitirá estructurar un Sistema de Gestión de Riesgos de TI que sea completo y cuente con el respaldo de las gerencias.

El proyecto planteado brindará pautas para el manejo de la información que permitan el control de los datos, no se pretende solventar la ausencia de un departamento de TI ni se busca eliminar al 100% la problemática de la empresa en esta área, pero si pretende ir alineando a esta en la cultura de la seguridad de la información y su gestión a través de tareas básicas y protocolos para subsanar aquellas áreas que durante el desarrollo de este proyecto se categoricen como críticas.

1.2.2 Problema General

¿Dispone SITEC Seguridad de la documentación pertinente para llevar a cabo la gestión de riesgos centrada en el manejo de la información de sus datos y el de sus clientes, con el propósito de reconocer y contrarrestar los riesgos asociados a la manipulación de la información empresarial que pudieran afectar la continuidad operativa de la empresa?

1.2.3 Problemas Específicos

¿Cuenta la empresa con protocolos o normas vigentes para la gestión de los diferentes incidentes que se puedan presentar con respecto a la gestión de riesgos de TI?

¿Los protocolos existentes (en caso de haberlos) se ajustan a la gestión actual de incidentes TI?

¿Existe un plan de gestión de seguridad de la información en SITEC Seguridad documentación para el manejo los datos dentro de la empresa?

¿Cuentan los colaboradores de la empresa con capacitaciones para la gestión de riesgos de TI?

1.3 Objetivo General Y Objetivos Específicos

1.3.1 Objetivo General

Desarrollar una propuesta para la implementación de protocolos basados en el marco COBIT 2019 para la gestión del departamento de TI de la empresa SITEC Seguridad. (Sistemas Integrados de Seguridad S.A.)

1.3.2 Objetivos Específicos

Diagnosticar las prácticas que SITEC Seguridad ha venido utilizando para la gestión de riesgos de TI.

Realizar un análisis de las prácticas, protocolos y procesos de seguridad de la información obtenidos durante el diagnóstico inicial de la empresa SITEC Seguridad para la creación de un manual interno de gestión de TI.

Desarrollar procedimientos para las mejores prácticas sobre la gestión de riesgos basado en la metodología del Marco de Gestión COBIT 2019

Implementar las normas del Manual mediante la capacitación del uso de metodologías desarrolladas, así como procedimientos documentados para la empresa SITEC Seguridad.

1.4 Alcance Y Limitaciones

1.4.1 Alcance Del Proyecto

- Proponer un mecanismo del proceso que va desde entender la realidad de una organización y la definición de estrategias para la gestión de riesgos de TI, hasta la implementación de un ciclo de gestión de riesgos.
- El mecanismo va a ser un apoyo y guía para mejores prácticas sobre el riesgo de la gestión de TI, no pretende hacerlo sino indicar como hacerlo, basándonos en recomendaciones existentes sobre la gestión de los datos y tomando en consideración los riesgos del manejo de la información.
- Para la propuesta metodológica se establecerá una base con las mejores prácticas del mercado relacionadas con la gestión del riesgo de TI basados en COBIT 5.

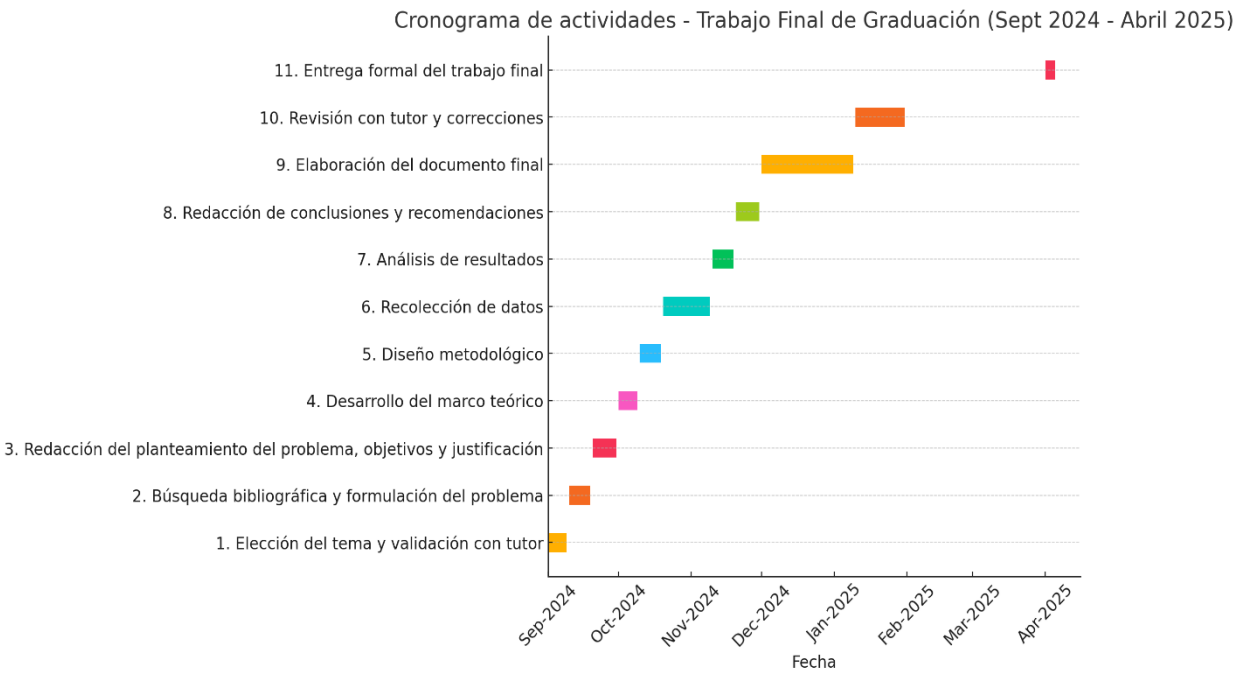
1.4.2 Limitaciones Del Proyecto

- Falta de documentación en la empresa.
- Disponibilidad limitada de horario para trabajar.
- Falta de concientización del manejo de los datos, complicaciones con la integración COBIT 2019, así como otros marcos para la gestión de riesgos de TI.
- Nula experiencia y documentación en la empresa, por causa de lo reciente que es COBIT 2019.

1.5 Cronograma De Actividades

- Nivel 1 Etapa 1: Planificación del proyecto
- Nivel 2 Definición de Objetivos
- Nivel 3 Investigación de Taxonomías
- Nivel 3 Definición de entregables
- Nivel 3 Redacción de Objetivos

Ilustración 1- Cronograma de actividades


Cronograma de actividades - Trabajo Final de Graduación (Sept 2024 - Abril 2025)
11. Entrega formal del trabajo final
10. Revisión con tutor y correcciones
9. Elaboración del documento final
8. Redacción de conclusiones y recomendaciones
7. Análisis de resultados
6. Recolección de datos
5. Diseño metodológico
4. Desarrollo del marco teórico
3. Redacción del planteamiento del problema, objetivos y justificación
2. Búsqueda bibliográfica y formulación del problema
1. Elección del tema y validación con tutor
Sep-2024
Oct-2024
Nov-2024
Dec-2024
Jan-2025
Feb-2025
Mar-2025
Apr-2025
Fecha

CAPÍTULO 2

MARCO TEÓRICO

Durante este capítulo se desarrollarán las definiciones de los diferentes conceptos que se utilizarán durante la creación de este proyecto, conceptos y definiciones importantes para el entendimiento de tanto de los lectores como de los funcionarios de la empresa.

Existen una serie de metodologías o de marcos regulatorios en temas de gestión de tecnologías de la información los cuales permiten a las organizaciones hoy en día a ser más productivas de acuerdo con los diferentes benchmarking que se hacen dentro de la gran cantidad de organizaciones, es ventaja competitiva utilizar estos marcos de referencia o también llamadas metodologías ágiles.

(Sánchez, 2014) nos dice: “Una mejor práctica es una forma de hacer las cosas o una serie de principios generalmente aceptados en un ámbito profesional, y que sirven para aportar valor de negocio; en el caso de las TI, a través del manejo de la información”, explicó Omar Sánchez, vicepresidente del IT Service Management Forum, dentro del marco de la Expo Tecnología 2014.

Sánchez dijo que, “a pesar de ser muchas y variadas, las mejores prácticas más comunes en TI son aquellas orientadas hacia la arquitectura empresarial, la gestión de servicios de TI, la gestión de riesgos de TI, la gestión de seguridad de la información y la gobernanza de TI.”

Existen puntos importantes dentro de las buenas prácticas como se indica, desde la forma de hacer las cosas hasta la adopción de normas, librerías y bibliotecas que permiten centralizar la información, ofreciendo procedimientos con resultados que aportan la gestión de servicios de TI, existen varias en el mercado como lo son ISO/IEC, COBIT 2019 y ITIL.

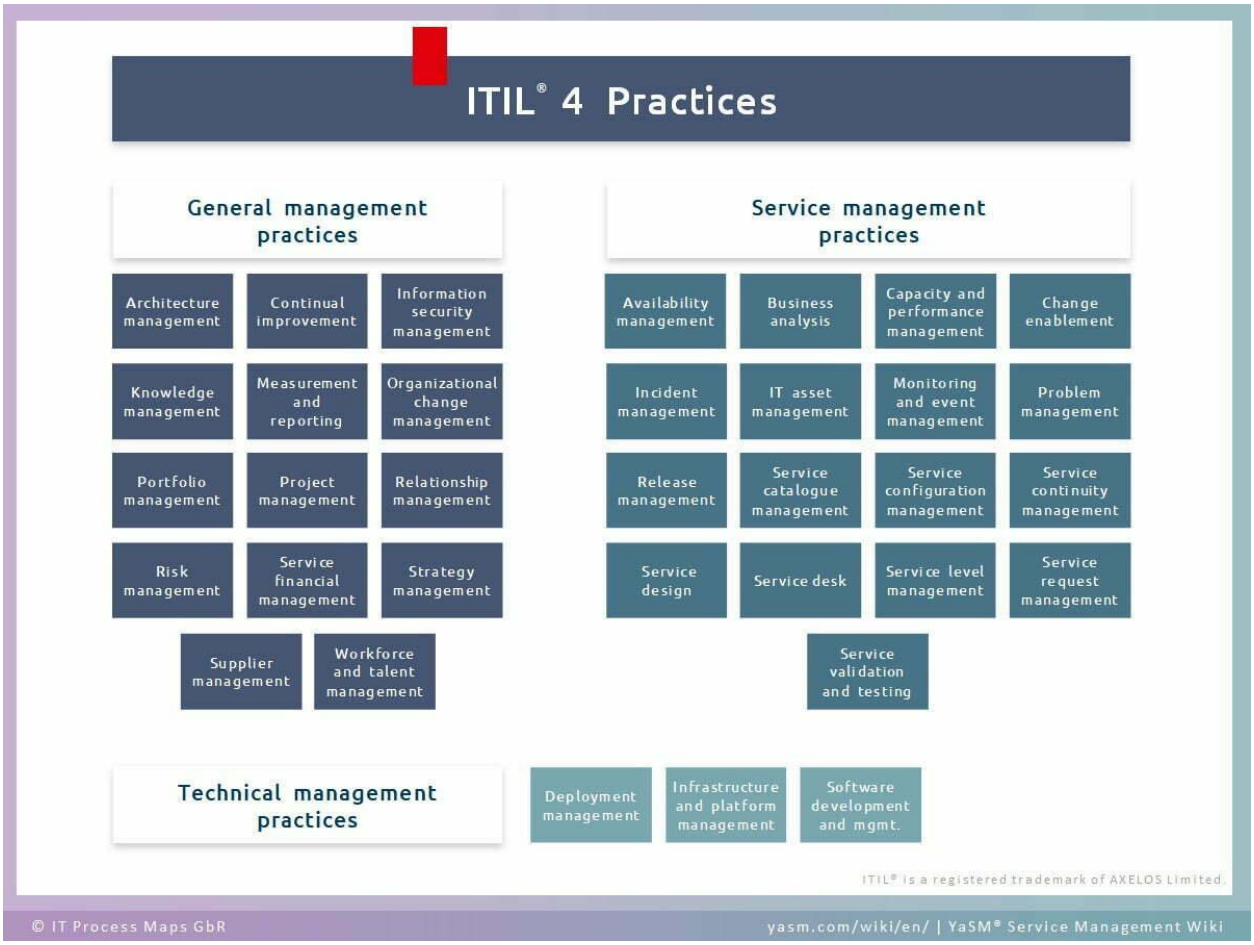
(IBM.COM, s.f.) nos define ITIL como: “Una biblioteca de mejores prácticas para gestionar servicios de TI y mejorar el soporte y los niveles de servicio de TI. Uno de los principales objetivos de ITIL es promover la alineación entre los servicios de TI y los objetivos comerciales, incluso a medida que cambian.”

En base en lo anterior ITIL es considerado un conjunto que permite la mejora de prácticas en la gestión de servicios de TI, basándose en propósitos de mejora a nivel de servicio, lo anterior hace que se centre en una metodología que pretende optimizar la entrega de servicios, permitiendo una mayor eficiencia y efectividad en las empresas.

ITIL a su vez promueve la alineación entre servicios de TI y los objetivos de las empresas, por lo cual debe existir una integración efectiva entre las estrategias de la empresa y las metas que la misma posee, asegurando a través de iniciativas e innovación tecnológica la propiciación de la adaptación ante el entorno en que se desarrolla, permitiendo de esa manera evolucionar y ajustarse a las nuevas demandas del mercado.

Se puede concluir que ITIL es un marco para la gestión de servicios de TI, utilizando una biblioteca de mejores prácticas que garantizan un soporte eficiente y efectivo con los objetivos comerciales de las empresas; su enfoque de adaptabilidad permite enfrentar desafíos actuales y prepararse para los futuros.

Ilustración 2- ITIL 4 Practices: General management practices, service management practices and technical management practices



Fuente:(proactivanet.com, s.f.)

(ADEN.ORG, 2024) nos dice:

"Las metodologías ágiles permiten cambiar las prioridades de cada fase del proyecto, según los objetivos y necesidades del cliente, y está orientada a obtener resultados tangibles desde el principio.

La metodología ***Agile*** ayuda en el desarrollo de proyectos que necesitan rapidez y flexibilidad para adecuarse a las necesidades del cliente. Siempre enfocada a mejorar resultados."

Se puede entender que las metodologías ágiles ofrecen enfoques flexibles y dinámicos para la gestión, permitiendo al equipo ajustarse a prioridades en cada fase según se definan los objetivos y necesidades del cliente, esta adaptación permite lograr resultados concretos desde el inicio y donde es crucial la rapidez y capacidad de respuestas.

Una característica de las metodologías agiles es la capacidad de poder descomponer o dividir el proyecto en partes pequeñas y manejables, lo que facilita la resolución en periodos cortos en una manera interactiva y a medida que se avanza, permitiendo así ajustarse de manera constante por la retroalimentación recibida de las partes involucradas, lo anterior contribuye a aumentar la eficiencia, productividad y colaboración entre el equipo y cliente; en las metodologías ágiles la comunicación abierta y continua es clave, ya que permite reaccionar ante cambios necesarios productos de nueva información suministrada.

Se entiende que las metodologías ágiles son un marco que ofrecen una mejor gestión de proyectos, optimizando y garantizando que las necesidades del cliente se alineen y adapten a un entorno de constante cambio y evolución,

Los marcos regulatorios se pueden definir como modelos, normas y estándares que permiten entender los procesos, así como mejorar de manera continua los servicios y productos, su objetivo es garantizar que las empresas se alineen con necesidades de clientes internos o externos, también estos marcos permiten a la clasificación u empresa de roles y procesos dentro de la empresa, implementando algunos mecanismos de monitoreo, medición, mejoras de procesos, garantizando la gestión, gobernabilidad y actividades de cumplimiento.

Estas regulaciones aseguran una gestión y gobernanza eficaz, adoptando estándares y normas en las empresas a través de prácticas dentro de un marco normativo y legal, que a su vez minimiza riesgos, fortaleciendo la confianza y reputación de la empresa. Además, facilitan y

mejoran procesos mientras garantizan la gestión y cumplimiento, ofreciendo excelencia y sostenibilidad a largo plazo de las empresas.

Dentro de las metodologías o marcos regulatorios en temas de gestión de tecnologías de la información tomaremos como base de este proyecto es COBIT 2019, según (ISACACR.ORG, 2024):

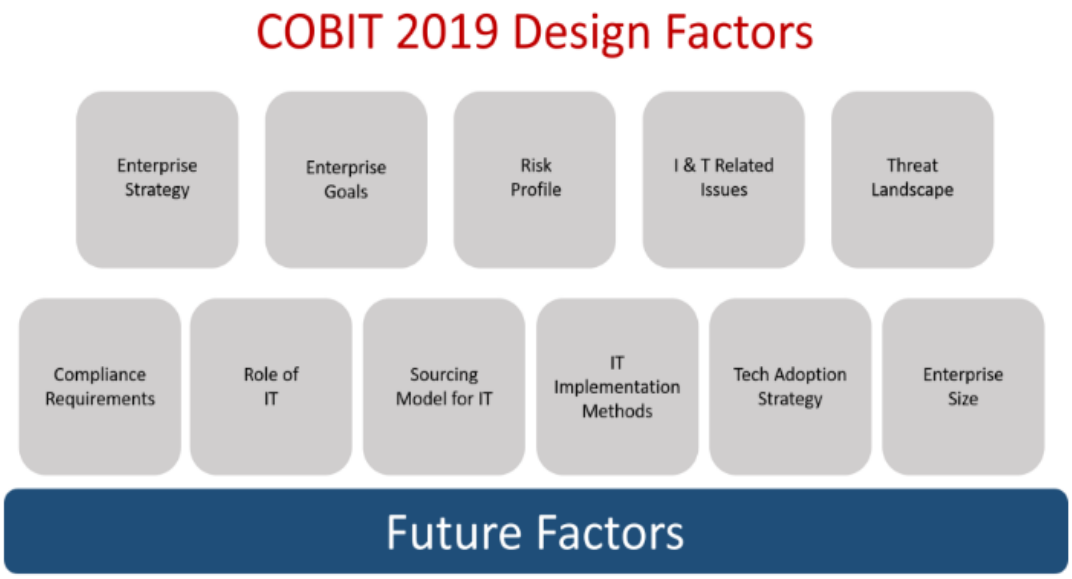
“el COBIT es un marco que apoya el gobierno de TI mediante la definición y la alineación de los objetivos de negocio con los objetivos de TI y procesos de TI.
Se puede definir también como un conjunto de los objetivos de control de tecnología de la información generalmente aceptadas, para la gestión de TI. El marco proporciona un conjunto de mejores prácticas para la gobernabilidad y el proceso de control de sistemas de información y tecnología con la esencia de la alineación de TI con el negocio.”

Con respecto a lo anterior se puede mencionar que COBIT 2019 se presenta como un marco que puede ser usado para el apoyo y gestión del gobierno de TI, lo hace mediante definiciones y alineando objetivos, procesos de TI con los empresariales, se puede entender que el marco son una serie de objetivos ampliamente aceptados y usados en la gestión de TI, todo esto a su vez va proporcionar las mejores prácticas para la gobernabilidad y control de sistemas de información, dándole un enfoque de seguridad de la TI totalmente alineada con la empresa y negocio.

Bajo ese contexto COBIT 2019 alinea todos aquellos objetivos dentro del marco de gestión de TI, está alineación permite de manera más coherente y efectiva gestionar la TI,

garantizando estrategias e implementaciones de enfoques que permiten optimizar y tener control del negocio basados en los procesos de TI.

Ilustración 3- COBIT 2019 DESIGN FACTORS



Fuente:(INVENSISLEARNING.COM, 2019)

El marco de gestión de TI, COBIT hace referencia también a las normas de ISO de seguridad, la información ISO de sistemas de gestión de seguridad información como el ISO 22301, ISO 27001 y también ISO 27002, de acuerdo con (ISOTools.ORG, 2022):

"ISO/IEC 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO/IEC 27001:2022 para los Sistemas Gestión de la Seguridad de la información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.”

Ilustración 4 - What are the new controls in ISO 27001 2022

Fuente:(ADVISERA.COM, 2022)

Se puede concluir de lo anterior que el ISO/IEC 27001 es un estándar o norma internacional que permite a las organizaciones tener un aseguramiento de la seguridad, teniendo

confidencialidad e integridad de su información, además ofrece un marco para los Sistemas de Gestión de la Seguridad de la Información (SGSI) a través de evaluaciones de riesgos y aplicando procesos y controles que permiten identificar, mitigar o eliminar los riesgos.

Esta norma no solo viene a mejorar la gestión de TI, sino que ofrece una ventaja competitiva a nivel de mercado para la empresa, ya que al ser certificable la empresa se diferenciara de los competidores, con lo cual ayuda a generar confianza y una imagen distinta frente a clientes.

Por otra parte la Gestión de la Seguridad de la Información está complementada con buenas prácticas y controles como lo recomienda la norma ISO 27002, la cual se basa en directrices, recomendaciones y buenas prácticas, juntas ambas normas forman y ofrecen un enfoque integral que ayudan a las empresas a dar seguridad a su información de manera efectiva con todos los desafíos que esto implica en un entorno que cada vez es más digitalizado, (ISO.ORG, 2022) nos dice que:

"ISO/IEC 27002:2022 –Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información, proporciona un conjunto de referencia de controles genéricos de seguridad de la información, incluida una guía de implementación. Aborda la ciberseguridad y protección de datos y ha evolucionado con respecto a su primera publicación en 2005. Ahora el contenido es más completo e integral y se basa en resiliencia, protección, defensa y gestión."

Con lo anterior se entiende que el ISO 27002 se enfoca en normas de seguridad de la información, la protección de datos y la ciberseguridad, ofreciendo un marco con controles,

directrices y prácticas que permitan implementarse de manera efectiva, la primera edición es del 2005 y se ha ampliado con temas críticos como la resiliencia, la defensa, la protección y gestión de la seguridad.

ISO 27002 proporciona practicas a través de estándares con un enfoque analítico de los procesos, la norma presenta 93 controles lo que permite a las empresas mejorar tras evaluar su seguridad, lo que resulta esencial para dar aseguramiento, confidencialidad, integridad y disponibilidad de la información.

Las empresas que adoptan esta norma fortalecen de manera proactiva la identificación y gestión de riesgos, creando confianza en clientes, donde un negocio cada vez más digitalizado y conectado enfrenta desafíos en el ámbito de la seguridad y ciberseguridad, es ahí donde la norma ISO 27002 tiene relevancia, proporcionando una guía con prácticas que ayudan a las empresas a enfrentar amenazas constantes, garantizando de manera más robusta y efectiva la gestión de la seguridad.

Ilustración 5- ISO 27002:2022 OVERVIEW

Fuente: (ISMS.ONLINE, 2022)

Por su parte (ISOTools.US, ISO 20000: ¿Por qué es buena idea implementarla en tu organizacion?, 2016)define ISO 20000 como “Una metodología con enfoque para gestionar los servicios TI y así demostrar que la organización hace uso de mejores prácticas”, podemos decir que ISO 2000 es una metodología esencial en la gestión de TI, la norma permite demostrar a las empresas buenas prácticas tras su adopción, dando no solo un estándar internacional, sino facilitando la mejora continua de procesos y servicios dentro de la empresa.

Las empresas logran subir la calidad de sus servicios al seguir las directrices de la norma ISO 20000, aumentando la satisfacción de clientes tras una gestión eficiente de los recursos,

planificando, gestionando incidentes y problemas con prácticas efectivas, la evaluación constante de los servicios, la identificación de mejoras y los cambios aplicados benefician a la empresa y clientes.

En un entorno cada vez más digitalizado la calidad y eficiencia es fundamental, la implementación de la norma ISO 20000 permite alcanzar el éxito a largo plazo, ofreciendo una base sólida para la gestión de TI de manera efectiva.

Ilustración 6- 5 BENEFICIOS ISO 20000

Fuente: (YASM.COM, 2024)

(ISOTools.US, Sistema de Gestión de Continuidad de Negocio, 2024) nos define:

"ISO 22301 como una norma internacional de gestión de continuidad de negocio.

ISO 22301 identifica los fundamentos de un Sistema de Gestión de la Continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio.

Proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de la organización. Se usa para asegurar a las partes interesadas clave que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente.

La norma proporciona a las organizaciones un marco que asegura que ellos pueden continuar trabajando durante las circunstancias más difíciles e inesperadas, siempre protegiendo a sus colaboradores, manteniendo su reputación y proporcionando la capacidad de continuar trabajando y comercializando.”

Se considera ISO 22301 como una norma que establece un proceso dando aseguramiento y la continuidad del negocio, la norma permite definir procesos, principios y términos para su implementación con un propósito solido en bases que permiten entender, desarrollar e implementar estrategias de continuidad ante circunstancias inesperadas, permitiendo estar preparados y sin dejar de lado el cumplimiento interno o externo de la organización.

ISO 22301 ofrece un marco integral que puede asegurar en gran medida a las empresas continuar operando en circunstancias imprevistas y desafiantes, lo cual implica priorizar, proteger a sus colaboradores, manteniendo la reputación de la empresa, así como asegurar la continuidad de las operaciones, no solo centrándose en cierta manera en la supervivencia de la empresa, sino también permitiendo a la misma adaptarse en situaciones adversas, en resumen ISO 22301 garantiza la continuidad del negocio, cumpliendo con obligaciones ante eventos inesperados lo que da confianza a sus clientes.

Ilustración 7- ISO 22301

Fuente:(HOBBS.UK, 2022)

(NORMASISO.ORG, s.f.) nos define: “La norma ISO 27032, también conocida como "Directrices para la ciberseguridad", establece los principios y las mejores prácticas para gestionar y mitigar los riesgos asociados a la ciberseguridad. Su objetivo es ayudar a las organizaciones a proteger sus sistemas de información y mantener la confidencialidad, integridad y disponibilidad de los datos.”

Con lo anterior se entiende que la norma establece principios y mejores prácticas para la gestión de los riesgos desde el punto de vista de la ciberseguridad, con un propósito claro, el proteger los sistemas de información de las empresas garantizando la confidencialidad, integridad y disponibilidad de todos los datos, la adopción permite a las empresas establecer marcos sólidos, promoviendo una cultura de prevención y preparación ante incidentes, en un entorno donde las amenazas cibernéticas son cada vez más frecuentes y sofisticadas, esta norma proporciona directrices claras para enfrentarse a la ciberseguridad a la vez que fortalece la

capacidad de las empresas para proteger la información todo visto desde un panorama digital que está en constante evolución.

La Norma se desarrolla en la gestión de 4 riesgos: prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje, los mismos son trabajados en fases como: el entendimiento de la empresa, el análisis de riesgos, un plan de acción y la implementación a través de controles a nivel de aplicación, servidores, usuarios finales y controles de ataques de ingeniería social.

Ilustración 8- Dominios de ISO/IEC 27032:2012

Fuente (HACKHISPANO:COM, 2012)

CAPÍTULO 3

MARCO METODOLÓGICO

(CONCEPTO.DE, 2024) Nos define “el marco metodológico es un apartado de los proyectos de investigación en el que se detallan los métodos de análisis colaboradores para abordar el objeto de estudio.”

El marco metodológico, se considera un elemento base de la investigación y el cual permitirá alcanzar un objetivo específico, incluyendo técnicas e instrumentos para la recolección de datos, en el desarrollo de esté se abarcará el enfoque de la investigación, fuentes de información, así como técnicas de recolección de la misma, lo anterior va ser crucial en la generación de datos relevantes y confiables.

Se explicarán las técnicas e instrumentos a utilizar para la generación y recolección de datos, asegurando información precisa y confiable, para posterior interpretar la misma y así presentar un procedimiento de análisis que permita el desarrollo de la propuesta de solución, podemos entender que el marco metodológico no solo guiará el proceso investigativo, sino que también va ser el responsable de proporcionar una estructura confiable que valide los resultados obtenidos.

Enfoque De La Investigación

(Sampieri, 2014) nos dice:

“Es: un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema.

A lo largo de la historia de la ciencia han surgido diversas corrientes de pensamiento (como el empirismo, el materialismo dialéctico, el positivismo, la fenomenología, el

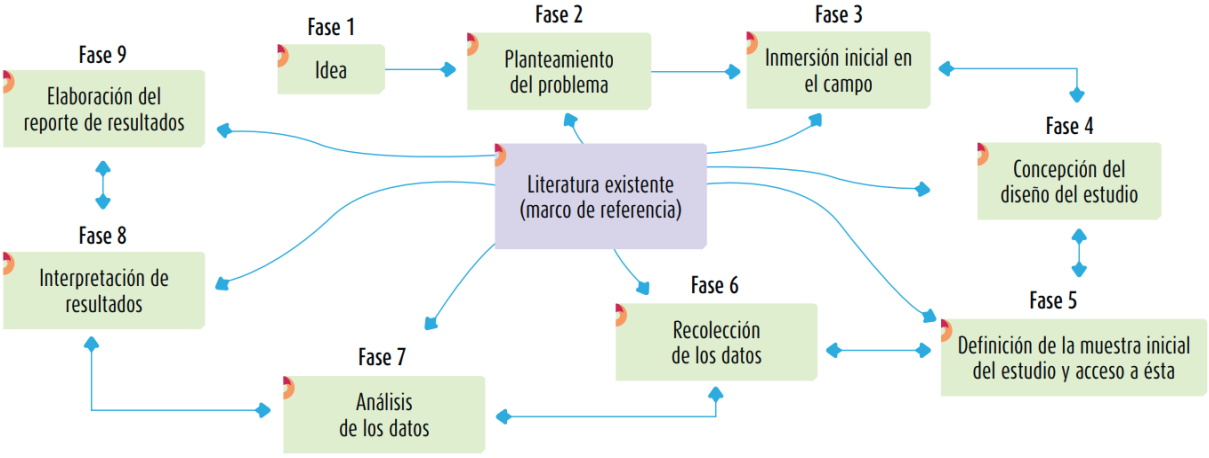
estructuralismo) y diversos marcos interpretativos, como el realismo y el constructivismo, que han abierto diferentes rutas en la búsqueda del conocimiento.”

Sin embargo, y debido a las diferentes premisas que las sustentan, desde el siglo pasado tales corrientes se “polarizaron” en dos aproximaciones principales de la investigación: el enfoque cuantitativo y el enfoque cualitativo.”

En base a lo anterior se puede indicar que la metodología de investigación es mixta pues llegará a utilizar investigación cualitativa, la cual se distingue por la capacidad de realizar un análisis profundo y detallado que permitirá ajustar los planteamientos de una manera flexible durante la investigación, este tipo de enfoque se centra en comprender y otorgar significado a los datos, lo cual resulta crucial y facilita una comprensión completa de los estudios realizados.

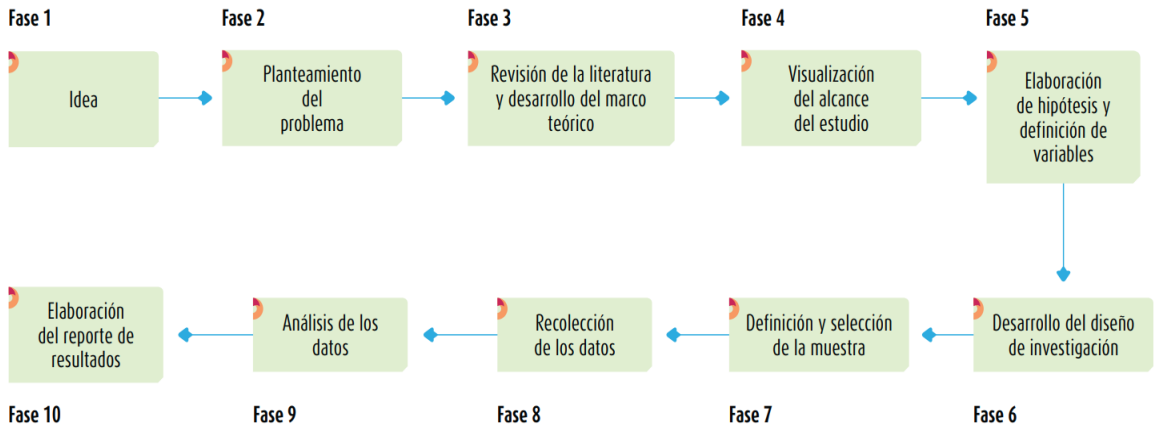
Mediante este enfoque los datos emergerán directamente de un cuestionario, los mismos serán analizados en función del contexto en el que se producen, permitiendo entender comportamientos y dinámicas en situaciones cotidianas de la empresa, de esta manera busca obtener una representación de la realidad.

Ilustración 9- Proceso cualitativo



A la vez la investigación posee es un enfoque cuantitativo porque será utilizado para el procesamiento los datos recolectados y con ello se podrá determinar los resultados necesarios a través de la medición y el análisis estadístico.

Ilustración 10- Proceso cuantitativo



(Sampieri, 2014) nos dice:

"Ambos enfoques emplean procesos cuidadosos, metódicos y empíricos en su esfuerzo para generar conocimiento, por lo que la definición previa de investigación se aplica a los dos por igual. En términos generales, estos métodos utilizan cinco estrategias similares y relacionadas entre sí (Grinnell,1997):

1. Llevan a cabo la observación y evaluación de fenómenos.

2. Establecen suposiciones o ideas como consecuencia de la observación y evaluación realizadas.

3. Demuestran el grado en que las suposiciones o ideas tienen fundamento.

4. Revisan tales suposiciones o ideas sobre la base de las pruebas o del análisis.

5. Proponen nuevas observaciones y evaluaciones para esclarecer, modificar y fundamentar las suposiciones e ideas o incluso para generar otras.

Sin embargo, aunque las aproximaciones cuantitativa y cualitativa comparten esas estrategias generales, cada una tiene sus propias características."

Fuentes De Información

Fuentes Primarias

Las fuentes de información primarias para este trabajo son las siguientes:

- El Marco COBIT 2019 y sus diferentes guías oficiales publicadas por ISACA.

- La norma INTE/ISO 27001:2022 y otras normas relacionadas con la gestión de riesgos y la gestión de tecnología de información.

- Libros sobre metodología de la investigación e investigación cualitativa.

Tipo de documento	Nombre del documento	Versión del documento	Año
Marco regulatorio	Control Objectives for Information Technologies – ISACA (COBIT 2019)	COBIT 2019	2019
Norma ISO	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	27001:2022	2022
Norma ISO	ISO/IEC 27002: 2022 Information security, cybersecurity and privacy protection — Information security controls	27002: 2022	2022
Manuales de Sitec Seguridad	Politicas de Ciberseguridad	Version 1	2024
Manuales de Sitec Seguridad	Acuerdo de confidencialidad	Version 2	2015
Manuales de Sitec Seguridad	Prohibición del uso del Celular	Versión 1	2024

Tabla 1- Fuentes Primarias

Fuentes Secundarias

Las fuentes secundarias de información utilizadas como apoyo para el desarrollo de este trabajo de graduación son de páginas de internet, informes, reportes, artículos y blogs.

Tipo documento	Nombre del documento	Versión	Autor	Año
Security Report	Eset Security Report	Security Report:2023	Eset	2023
Auditoría interna	Auditoría normas COBIT 4.1	Auditoria:2009	Ivana Soledad Rojas Córsico	2009
Blog	Sistema de gestión de denuncias: elemento clave para la gobernanza de las organizaciones	INTE/ISO 37002:2021	Inteco	2021
Blog	La norma 27001 y su importancia en seguridad de la información IT	INTE/ISO/IEC 27001:2021	Inteco	2021
Documento	Acuerdo de confidencialidad	Versión 2	Sitec Seguridad	2015
Documento	Política de Ciberseguridad	Versión 1	Sitec Seguridad	2022
Documento	Prohibición del uso del Celular	Versión 1	Sitec Seguridad	2024

Tabla 2- Fuentes Secundarias

Sujetos De Información

Como parte del proceso de investigación para el presente trabajo, se destaca la participación y colaboración activa del grupo de trabajo de Sitec Seguridad, estos colaboradores juegan un papel importante a lo largo del proceso, permitiendo la recolección de datos para así lograr la elaboración de la propuesta metodológica, con estos actores permitirá obtener una visión amplia y precisa de las prácticas actuales y necesidades lo que permitirá crear una propuesta sólida y alineada a las realidades de Sitec Seguridad, de acuerdo con la tabla 3 los sujetos de información aportarán información clave basada en su experiencia y conocimientos.

Tabla 3- Sujetos de Información

Nombre	Puesto	Profesión	Experiencia	Funciones/ roles
Jorge Sancho	Administrador	Administrador de Empresas	14 años	Administración general de la empresa
Irian Hernandez	Contadora	Contadora	6 años	Contabilidad y apoyo administrativo
Alexis Valverde	Ventas	Técnico en Seguridad	14 años	Ventas de la compañía, visitas
Maria Chinchilla	Administrativo	Estudiante de Derecho	5 años	Funciones administrativo, apoyo contable

Natalia Solís	Administrativo	Asistente administrativa	1 años	Funciones administrativo, apoyo contable
Roy Goméz	Técnico Supervisor	Técnico en Seguridad	6 años	Instalaciones, supervisión
Ruddy Jimenez	Técnico	Técnico en Seguridad	5 años	Instalaciones
Julio León	Técnico	Técnico en Seguridad	5 años	Instalaciones
Harlinton Obando	Técnico	Técnico en Seguridad	3 años	Instalaciones
Cristian Morales	Técnico	Técnico en guridad	1 año	Instalaciones
Cristian Sancho	Técnico	Técnico en Seguridad	1 año	Instalaciones
Daniel Sancho	Técnico	Técnico en Seguridad	1 año	Instalaciones
Carlos Piñeres	Técnico	Técnico en Seguridad	1 año	Instalaciones
Juan Murillo	Técnico	Técnico en Seguridad	1 año	Instalaciones
Jesús Benavides	Técnico	Técnico en Seguridad	1 año	Instalaciones
William Gonzalez	Técnico	Técnico en Seguridad	1 año	Instalaciones
Lesvin Vega	Técnico	Técnico en Seguridad	1 año	Instalaciones

Fuente: elaboración propia

Técnicas De Recolección De Datos

Para recopilar la información mencionada, se utilizará una serie de métodos cualitativos, los cuales se describen en la siguiente sección.

El desarrollo de este trabajo se utilizarán algunas herramientas de Microsoft Office o Microsoft Office 365, para la creación de cuestionarios a los involucrados se utilizará encuestas digitales a traces de Google Forms, donde se aplicará: Cuestionarios, entrevistas, observación, observación por medio de investigación de campo.

(Sampieri, 2014) nos define “Cuestionario conjunto de preguntas respecto de una o más variables que se van a medir”, se puede entender que el cuestionario como tal está considerado como una de las herramientas más utilizadas en la recolección de datos, esto gracias a su capacidad de obtener información de manera organizada y estructurada, se compone de una serie de preguntas con el fin de obtener respuestas específicas sobre una o varias variables a analizar, es común utilizarlo en diversas áreas de investigación.

Las preguntas del cuestionario estarán formuladas de tal manera que facilitarán la obtención de datos cuantitativos y cualitativos, las preguntas pueden ser cerradas, con respuestas predeterminadas, o abiertas, con lo que se permitirá a los participantes proporcionar respuestas más detalladas.

El cuestionario tiene la particularidad de ser aplicado en diversos formatos, como papel, en línea o de manera presencial, lo que le da una gran flexibilidad al instrumento y lo hace adecuado para distintas situaciones y poblaciones. Finalizamos mencionando su capacidad para

generar datos precisos y confiables lo que lo convierte en una herramienta clave para obtener información valiosa en investigaciones.

A su vez (Sampieri, 2014) define la entrevista “reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados), por lo anterior la entrevista está considerada como una herramienta fundamental para la recolección de datos gracias a su naturaleza interactiva y flexible, lo que nos permite un intercambio de información directo entre el entrevistador y los entrevistados, logrando una visión más completa sobre el tema tratado. El entrevistador formulará preguntas, guía durante la conversación y los entrevistados a través de sus respuestas, aportan conocimientos y experiencias de tema consultado.

La entrevista hace que sea utilizada gracias a su versatilidad, teniendo los objetivos y la estructura correcta las entrevistas serán organizadas, lo que ofrece diferentes ventajas, podemos decir que las entrevistas estructuradas, nos aseguran cobertura de todos los temas de una manera consistente, mientras que las no estructuradas ofrecen un flujo más libre, propiciando mayor espontaneidad en las respuestas.

(Sampieri, 2014) nos define “Observación cualitativa, no es mera contemplación (“sentarse a ver el mundo y tomar notas”); implica adentrarnos profundamente en situaciones sociales y mantener un papel activo, así como una reflexión permanente. Estar atento a los detalles, sucesos, eventos e interacciones.”

Con lo anterior se entiende que la observación cualitativa está presente como un proceso complejo y es más de lo que parece a simple vista, ya que no se trata solamente de observar

pasivamente y tomar notas como nos dice Sampieri, sino que requiere que el observador o investigador se adentre activamente en las situaciones, interactuando directamente con el entorno y los participantes, de esta manera se está en una reflexión constantemente de lo que se está observando, permitiendo entender el significado de las acciones y de los eventos que ocurren, permitiendo obtener una visión profunda del contexto que se está observando.

Adicionalmente, el observador debe prestar atención a los detalles pequeños y sutiles que podrían pasar por desapercibidos, ya que son clave para una comprensión más completa del fenómeno en cuestión, se deben observar interacciones entre las personas, cambios de ambiente, gestos y hasta las actitudes, con lo cual de esta manera, se obtendrá una perspectiva detallada permitiendo captar matices importantes, los cuales enriquecen la interpretación de los datos y proporcionan una visión precisa y completa de la realidad observada.

Variables De La Investigación

Tabla 4-Variables de la investigación

Objetivos específicos	Variables asociadas	Descripción	Indicador
Diagnosticar las prácticas de Seguridad utilizadas para la gestión de riesgos de TI.	Controles de referencia del marco COBIT 2019	Diagnosticar las prácticas para la gestión de riesgos de TI	Los controles aplicables del marco COBIT 2019 – ISO 27001:2022 | 27002:2022
Realizar un análisis de las prácticas, protocolos y	Revisión de los controles para la	Análisis de los controles	Los controles aplicables del marco

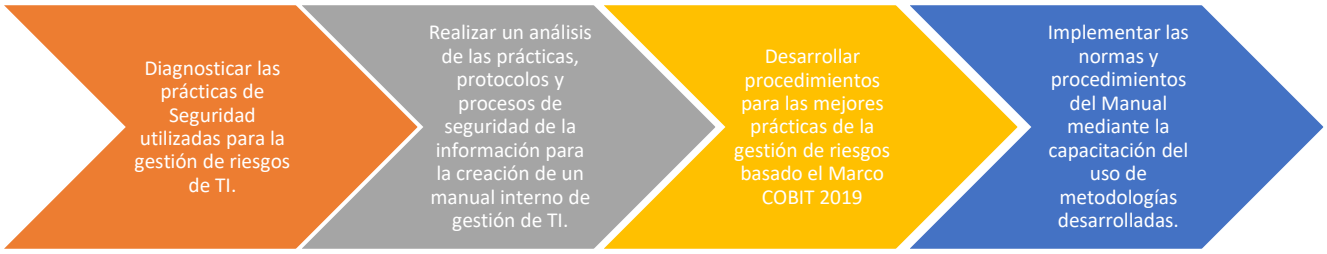
procesos de seguridad de la información obtenidos durante el diagnóstico inicial de la empresa SITEC Seguridad para la creación de un manual interno de gestión de TI.	creación de un manual interno	existentes para validación con el marco COBIT 2019	COBIT 2019 – ISO 27001:2022 | 27002:2022
Desarrollar procedimientos para las mejores prácticas sobre la gestión de riesgos basado en la metodología del Marco de Gestión COBIT 2019	Diseño y desarrollo de la propuesta de procedimientos para las mejores prácticas en gestión de riesgos	Creación de procedimientos para la gestión de riesgos basados en la metodología marco de gestión COBIT 2019	Los controles aplicables del marco COBIT 2019
Implementar las normas del Manual mediante la capacitación del uso de metodologías desarrolladas, así como procedimientos	Ejecución de la propuesta para la implementación de controles	Implementación de los controles desarrollados, utilizando la metodología del marco de gestión COBIT 2019	Los controles aplicables del marco COBIT 2019

documentados para la empresa SITEC Seguridad.			

Fuente: elaboración propia

Diseño De La Investigación

Ilustración 11 - Diseño de la investigación



Fuente: elaboración propia

Fase 1

El primer paso del proceso consiste en realizar un diagnóstico de las prácticas de seguridad utilizadas en la gestión de riesgos de TI de la empresa Sitec Seguridad, este análisis implica una revisión detallada de las prácticas que la empresa utiliza, ha implementado para identificar y gestionar los riesgos tecnológicos, con el propósito de evaluar su efectividad y enfoque.

Durante esta fase 1 se procederá a verificar si las prácticas adoptadas, con la finalidad de identificar si están debidamente reguladas y alineadas con el marco normativo COBIT 2019, está

revisión permitirá evaluar si las medidas adoptadas cumplen con los estándares y directrices necesarios para una adecuada gestión de los riesgos tecnológicos dentro de la empresa.

Fase 2

Tiene como objetivo el análisis y revisión profunda de las prácticas, protocolos y procesos de seguridad de la información, con el fin de desarrollar un manual en la siguiente fase para la gestión de TI en la empresa Sitec Seguridad, con este análisis se elaborará una propuesta integral que abarque las áreas relacionadas con la gestión de riesgos tecnológicos.

El proceso de análisis durante la fase 2 implicará una comparación de las prácticas identificadas en el diagnóstico y los procesos, con el propósito de determinar cuáles pueden mantenerse tal como están, cuáles deben ser modificadas y cuáles no existen en base al marco COBIT 2019, de esta evaluación se integrarán las prácticas más recomendadas en el diseño de una propuesta que abarcará el desarrollando los procedimientos que garanticen su efectividad y alineación con las necesidades de la empresa.

Fase 3

En esta fase se utilizará toda la información recopilada y obtenida en las fases anteriores, con el fin de desarrollar una propuesta de procedimientos que se ajuste a las mejores prácticas en la gestión de riesgos, dicha propuesta estará basada en el marco COBIT 2019, lo que garantizará que el enfoque para implementar los procedimientos sea organizado y coherente con las necesidades de Sitec Seguridad.

El proceso de desarrollo de procedimientos estará centrado en aplicar las mejores prácticas de gestión de riesgos, tomando como referencia principal el marco COBIT 2019, lo que permitirá procedimientos alineados con los estándares, así como principios establecidos por dicho marco, asegurando su consistencia e efectividad.

Fase 4

En esta última fase se llevará a cabo el proceso de implementación los procedimientos aplicando las normas, a través de la capacitación de los usuarios de la empresa Sitec Seguridad en el uso de las metodologías diseñadas, el manual desarrollado en la fase anterior se utilizará como herramienta central para este proceso formativo de los usuarios y que será presentado para su evaluación.

La implementación de las normas y procedimientos basados en el marco COBIT 2019 garantizará mediante una capacitación efectiva y asegurando que los usuarios comprendan las mismas, logrando aplicar correctamente las metodologías establecidas, todo el proceso estará basado en el manual creado y con el cual se proporcionará las directrices necesarias para su correcta ejecución.

Matriz De Coherencia

Tabla 5 - Matriz de coherencia

Objetivos	Entregable	Fase del proyecto	Técnicas de recolección	Instrumentos utilizados	Relación con el marco teórico
Diagnosticar las prácticas que SITEC Seguridad ha venido utilizando para la gestión de riesgos de TI.	Diagnóstico inicial de las practicas utilizadas para la gestión de TI para la empresa Sitec Seguridad.	Fase 1: Se refiere al desarrollo del diagnóstico de las practicas utilizadas para la gestión de riesgos de TI.	Entrevistas, conversaciones con colaboradores de la empresa.	Observación, entrevistas, formularios.	Marco COBIT 2019 ISO 27001 ISO 27002
Realizar un análisis de las prácticas, protocolos y procesos de seguridad de la información	Listado de las prácticas actuales en comparativo con	Fase 2: Análisis de las prácticas, protocolos y procesos de	Entrevistas, conversaciones con colaboradores de la empresa.	Observación, entrevistas, formularios.	Marco COBIT 2019 ISO 27001 ISO 27002

obtenidos durante el diagnóstico inicial de la empresa SITEC Seguridad para la creación de un manual interno de gestión de TI.	el marco COBIT 2019 .	seguridad de la información para la creación de un manual interno de gestión de TI.			
Desarrollar procedimientos para las mejores prácticas sobre la gestión de riesgos basado en la metodología del Marco de Gestión COBIT 2019.	Propuesta de procedimientos, procesos y protocolos.	Fase 3: Desarrollo de las políticas, procesos y procedimientos para las mejores prácticas de la gestión de riesgos	Conversaciones con personal a cargo de la gestión de la información.	Marco COBIT 2019	Marco COBIT 2019 ISO 27001 ISO 27002

		basado el Marco COBIT 2019.			
Implementar las normas del Manual mediante la capacitación del uso de metodologías desarrolladas, así como procedimientos documentados para la empresa SITEC Seguridad.	Manual de procesos y procedimientos.	Fase 4: Implementación mediante el manual de capacitación para los usuarios de Sitec Seguridad.	Conversaciones con personal a cargo de las capacitaciones.	Marco COBIT 2019	Marco COBIT 2019 ISO 27001 ISO 27002

Fuente: elaboración propia

Durante este capítulo se brindaron las definiciones y se establecieron los enfoques de la investigación, así como la metodología que orientará la investigación del proyecto, este tuvo como objetivo sentar una base sólida, tanto en el ámbito teórico como práctico de manera que pueda garantizar que el estudio se realice de una manera ordenada y eficaz.

Se clarificaron los pasos a seguir y con ello se logrará estructurar un proceso investigativo de forma coherente y bien definida para el desarrollo de la propuesta final e implementación de la misma; en este capítulo se detallaron todos los entregables esperados al final del proyecto, proporcionando una visión clara de los resultados que deben alcanzarse en el mismo.

Se especificaron cada una de las fases del proyecto, las cuales serán una guía en el desarrollo de cada etapa, según el orden correspondiente, sin dejar de lado la identificación de los instrumentos que se utilizarán para toda la recopilación de datos, la ejecución de las actividades, con lo que se garantizará que el proceso se ejecute de acuerdo con los objetivos planteados y de forma sistemática.

CAPÍTULO 4

DIAGNÓSTICO

En este capítulo se plantean tres diagnósticos fundamentales para evaluar el estado actual de la empresa Sitec Seguridad en relación con la gestión de las tecnologías de la información, estos diagnósticos se enfocarán en áreas clave de la organización, proporcionando una visión integral de cómo se están manejando las tecnologías de la información y permitiendo identificar qué áreas requieren atención o mejoras.

El primer diagnóstico que se realizará será desde un enfoque administrativo, en el cual se revisarán, verificarán los procedimientos, protocolos y prácticas implementadas por la empresa en cuanto a la gestión de las TI, el diagnóstico incluirá una revisión de los documentos y/o manuales existentes de la empresa, así como una evaluación sobre el cumplimiento de las normativas y directrices que guían la gestión de TI en la empresa, con este primer diagnóstico se identificarán las posibles brechas o deficiencias en los procesos actuales, facilitando la determinación de las áreas que necesitan ajustes.

El segundo diagnóstico está más enfocado en los activos de la empresa desde el punto de vista tecnológico, abarca el software y el hardware en el cual se gestiona y almacenan la información actualmente, se realizará un inventario de los activos tecnológicos actuales, evaluando estado, eficiencia y capacidad, también se analizará la infraestructura física, incluido los servidores, centros de datos, topologías de rede y cualquier componentes de la planta física que juegan un papel crucial en la gestión de la información.

El tercer y último diagnóstico se basa en la percepción de los colaboradores de la empresa, y a través de entrevistas o cuestionarios previamente desarrollados se podrá obtener la opinión de los procesos y prácticas actuales en la gestión de la información, las preguntas de dicho cuestionario estarán orientadas a evaluar la percepción y la efectividad de las herramientas

o sistemas actuales, así como conocer el conocimiento y cumplimiento de los protocolos establecidos en la empresa, lo que será vital para identificar todas aquellas áreas de mejora donde se interactúan directamente con las TI en su día a día.

Diagnóstico

Diagnóstico Administrativo

Diagnóstico inicial de las practicas utilizadas para la gestión de TI para la empresa Sitec Seguridad. Imágenes de documentación existente por parte de le empresa.

Acuerdo de confidencialidad para manejo de la información Sitec Seguridad

Ilustración 12- Acuerdo de confidencialidad

SITEC SEGURIDAD

Acuerdo de confidencialidad para colaboradores

Entre nosotros, **Sitec Sistemas Integrados de Seguridad S.A.** cédula jurídica número representada en este acto por con cédula de identidad número en su condición de Representante Legal, y que en lo sucesivo para efectos de este acuerdo se denominará,**"SITEC SEGURIDAD** , y en este acto y que en lo sucesivo se denominará **"EL COLABORADOR",** hemos convenido en celebrar el presente Acuerdo de Confidencialidad, en adelante "ACUERDO".

Para efectos de este ACUERDO, se define EMISOR a la parte de este ACUERDO, sea **SITEC SEGURIDAD**, que provee información y RECEPTOR a la otra parte de este ACUERDO, sea el **COLABORADOR**, que la recibe.

Considerando que el EMISOR revelará o divulgará al RECEPTOR información de la empresa y/o de sus CLIENTES o tendrá acceso a la misma y que dicha información es considerada confidencial o privada para el EMISOR y sus CLIENTES, ambas partes han acordado establecer el presente ACUERDO y respetarlo por sus términos, el cual se regirá por la legislación vigente de acuerdo a las siguientes cláusulas y estipulaciones:

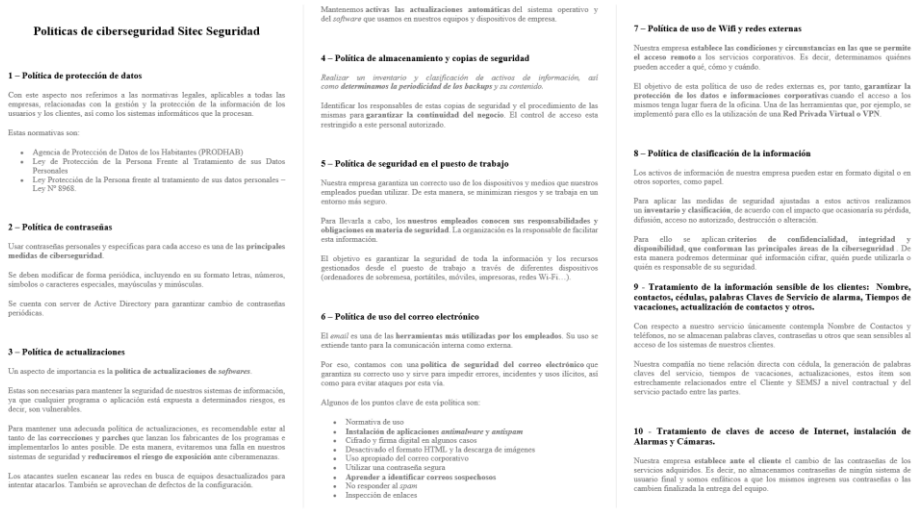
1. El RECEPTOR declara que tienen plenas facultades y capacidad para firmar, ejecutar y cumplir el presente Acuerdo.
2. Toda información que en cualquier forma se suministrada al RECEPTOR por parte del EMISOR y/o sus clientes el RECEPTOR deberá tratarla de manera confidencial según se estipula en el presente Acuerdo, sin tener en consideración si el EMISOR a la hora de su divulgación le dio el carácter de confidencial o privado, esta información no podrá ser divulgada en ningún momento de la relación laboral ni aun en el caso que dicha relación sea finalizada, la información no se podrá divulgar a ninguna persona incluyendo compañeros de trabajo que no estén autorizados a recibir dicha información.
3. Para efectos de este Acuerdo, se entiende por información confidencial (colectivamente denominada la INFORMACIÓN) toda información escrita, oral, gráfica o contenida en medios escritos, ópticos o electromagnéticos que incluye, información técnica, de seguridad, financiera, de negocios o comercial; procesos, capacidades operacionales y de procesamiento, métodos de transacción, información actual o futura, precios, costos, ventas, proyecciones de mercado o margen de ganancias; utilización de sistemas, programas y equipos de cómputo; información de investigación y desarrollo; listas de clientes y de Proveedores (actuales, potenciales y/o futuras); estrategias de negocios, estructura organizacional y composición de la sociedad, así como secretos industriales y comerciales, marcas y patentes (o aplicaciones de patentes), ideas (sean estas patentables o no), productos, servicios, derechos de autor, materiales, bases de datos, reportes, registros, diseños, planos, dibujos propiedad del EMISOR o de sus CLIENTES, así como de terceros

Fuente: Sitec Seguridad

Se encuentra una política o acuerdo de confidencialidad para los colaboradores, la cual regula la manera de cómo trabajar la información de los clientes, la manera correcta de almacenarla y/o compartirla sin exponer al cliente y a la empresa.

Política de ciberseguridad Sitec Seguridad

Ilustración 13- Política de ciberseguridad



Políticas de ciberseguridad Sitec Seguridad

1 – Política de protección de datos

Con este aspecto nos referimos a las normativas legales, aplicables a todas las empresas, relacionadas con la gestión y la protección de la información de los usuarios y los clientes, así como los sistemas informáticos que la procesan.

Estas normativas son:

- Agencia de Protección de Datos de los Habitantes (PRODHAB)
- Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales
- Ley Protección de la Persona frente al tratamiento de sus datos personales – Ley Nº 8968.

2 – Política de contraseñas

Usar contraseñas personales y específicas para cada acceso es una de las **principales medidas de ciberseguridad**.

Se deben modificar de forma periódica, incluyendo en su formato letras, números, símbolos o caracteres especiales, mayúsculas y minúsculas.

Se cuenta con server de Active Directory para garantizar cambio de contraseñas periódicas.

3 – Política de actualizaciones

Un aspecto de importancia es la **política de actualizaciones de *softwares***.

Estas son necesarias para mantener la seguridad de nuestros sistemas de información, ya que cualquier programa o aplicación está expuesta a determinados riesgos, es decir, son vulnerables.

Para mantener una adecuada política de actualizaciones, es recomendable estar al tanto de las **correcciones** y **parches** que lanzan los fabricantes de los programas e implementarlos lo antes posible. De esta manera, evitaremos una falla en nuestros sistemas de seguridad y **reduciremos el riesgo de exposición** ante ciberamenazas.

Los atacantes suelen escanear las redes en busca de equipos desactualizados para intentar atacarlos. También se aprovechan de defectos de la configuración.

Mantenemos **activas las actualizaciones automáticas** del sistema operativo y del *software* que usamos en nuestros equipos y dispositivos de empresa.

4 – Política de almacenamiento y copias de seguridad

*Realizar un inventario y clasificación de activos de información, así como **determinamos la periodicidad de los backups** y su contenido.*

Identificar los responsables de estas copias de seguridad y el procedimiento de las mismas para **garantizar la continuidad del negocio**. El control de acceso esta restringido a este personal autorizado.

5 – Política de seguridad en el puesto de trabajo

Nuestra empresa garantiza un correcto uso de los dispositivos y medios que nuestros empleados puedan utilizar. De esta manera, se minimizan riesgos y se trabaja en un entorno más seguro.

Para llevarla a cabo, los **nuestros empleados conocen sus responsabilidades** y **obligaciones en materia de seguridad**. La organización es la responsable de facilitar esta información.

El objetivo es garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de trabajo a través de diferentes dispositivos (ordenadores de sobremesa, portátiles, móviles, impresoras, redes Wi-Fi…).

6 – Política de uso del correo electrónico

El *email* es una de las **herramientas más utilizadas por los empleados**. Su uso se extiende tanto para la comunicación interna como externa.

Por eso, contamos con una **política de seguridad del correo electrónico** que garantiza su correcto uso y sirve para impedir errores, incidentes y usos ilícitos, así como para evitar ataques por esta vía.

Algunos de los puntos clave de esta política son:

- Normativa de uso
- **Instalación de aplicaciones *antimalware* y *antispam***
- Cifrado y firma digital en algunos casos
- Desactivado el formato HTML y la descarga de imágenes
- Uso apropiado del correo corporativo
- Utilizar una contraseña segura
- **Aprender a identificar correos sospechosos**
- No responder al *spam*
- Inspección de enlaces

7 – Política de uso de Wifi y redes externas

Nuestra empresa **establece las condiciones y circunstancias en las que se permite el acceso remoto** a los servicios corporativos. Es decir, determinamos quiénes pueden acceder a qué, cómo y cuándo.

El objetivo de esta política de uso de redes externas es, por tanto, **garantizar la protección de los datos e informaciones corporativas** cuando el acceso a los mismos tenga lugar fuera de la oficina. Una de las herramientas que, por ejemplo, se implementó para ello es la utilización de una **Red Privada Virtual o VPN**.

8 – Política de clasificación de la información

Los activos de información de nuestra empresa pueden estar en formato digital o en otros soportes, como papel.

Para aplicar las medidas de seguridad ajustadas a estos activos realizamos un **inventario y clasificación**, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración.

Para ello se aplican **criterios de confidencialidad, integridad** y **disponibilidad, que conforman las principales áreas de la ciberseguridad**. De esta manera podremos determinar qué información cifrar, quién puede utilizarla o quién es responsable de su seguridad.

9 - Tratamiento de la información sensible de los clientes: Nombre, contactos, cédulas, palabras Claves de Servicio de alarma, Tiempos de vacaciones, actualización de contactos y otros.

Con respecto a nuestro servicio únicamente contempla Nombre de Contactos y teléfonos, no se almacenan palabras claves, contraseñas u otros que sean sensibles al acceso de los sistemas de nuestros clientes.

Nuestra compañía no tiene relación directa con cédula, la generación de palabras claves del servicio, tiempos de vacaciones, actualizaciones, estos ítem son estrechamente relacionados entre el Cliente y SEMSJ a nivel contractual y del servicio pactado entre las partes.

10 - Tratamiento de claves de acceso de Internet, instalación de Alarmas y Cámaras.

Nuestra empresa **establece ante el cliente** el cambio de las contraseñas de los servicios adquiridos. Es decir, no almacenamos contraseñas de ningún sistema de usuario final y somos enfáticos a que los mismos ingresen sus contraseñas o las cambien finalizada la entrega del equipo.

Fuente: Sitec Seguridad

Dentro de la empresa Sitec Seguridad existe una política ciberseguridad, la misma regula la manera y el trato a los datos, contratistas, actualizaciones de equipos, almacenamiento y copias de seguridad, seguridad para puesto de trabajo, uso correo electrónico, uso de wifi y redes externas, clasificación de la información, entre otros, la misma aporta ideas cortas, claras y puntuales de que debería hacerse, mas no es muy extenso el desarrollo de las misma.

Política de uso celular

Ilustración 14- Política uso celular

SITEC SEGURIDAD

SITEC SEGURIDAD

PROHIBICIÓN DEL USO DEL CELULAR EN HORARIO LABORAL

PREPARADO POR: Maria Fernanda Chinchilla	**REVISADO Y APROBADO POR:** Iriam Hernández
FECHA: Octubre 2024	**PERIODOS DE REVISIÓN:** anual
PROXIMA REVISIÓN: Octubre 2025	**CONSECUTIVO:** SIT-2024-008

24 de octubre del 2024

Comunicado Oficial

Estimados colaboradores, por medio de la presente les informamos que, por disposición de la gerencia,

Fuente: Sitec Seguridad

La empresa posee una política sobre el uso del celular para los colaboradores, la cual regula el tiempo de uso, el motivo de uso, la información que se accede, con el fin de proporcionar una guía correcta de uso sin exponer la información del cliente y de la empresa a través del uso del mismo.

Diagnostico Técnico

La empresa posee actualmente riesgos que fueron identificados en el desarrollo del capítulo cuatro, los cuales permitirán a la gerencia tomar decisiones sobre los controles a implementar en el capítulo 5, los riesgos se muestran en la siguiente matriz:

Tabla 6 - Matriz de riesgos

presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objetivo es ue la empresa Sitec Seguridad cuente con una referencia a la hora de completar la información en las tablas de procesos.

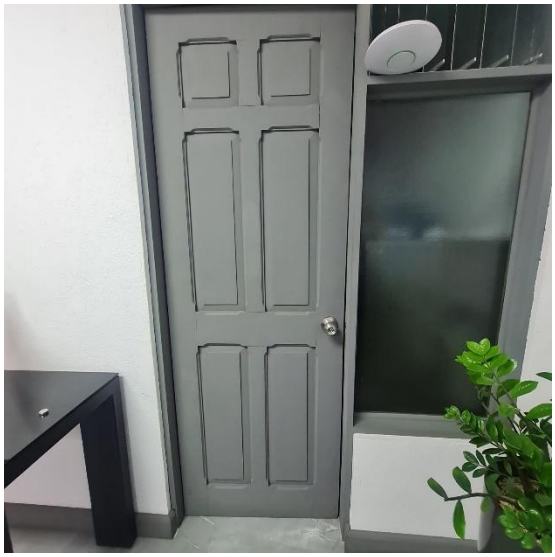
	PORTAFOLIO DE RIESGOS NORMATIVA TECNOLOGÍAS DE LA INFORMACIÓN
CODIGO	RIESGOS EN SEGURIDAD DE LA INFORMACIÓN
RS01	Incumplimiento de políticas de seguridad
RS02	Falta de capacitación y concientización en seguridad de la información
RS03	Políticas de seguridad no documentadas o están desactualizadas
RS04	Normativa de seguridad no documentadas o están desactualizadas
RS05	Controles de seguridad no documentados o están desactualizados
RS06	Procedimientos de seguridad no documentados o están desactualizados
RS07	Procesos de seguridad no documentados o están desactualizados
RS08	ataques de negación de servicios
RS09	No se actualiza en forma adecuada la plataforma tecnológica que atiende los servicios de internet
RS10	Plataforma de seguridad mal atendida, monitoreo inadecuado de incidentes de seguridad
RS11	Inadecuada en ingeniería social
RS12	Perdida de equipos de cómputo (principalmente portátiles) sin la debida protección, con la consiguiente pérdida de información confidencial.
RS13	Perfiles de acceso no definidos o mal configurados
RS14	Red interna puede ser vulnerada por parte de cibercriminales
RS15	gestión inadecuada en el parchado de aplicaciones o equipos
CODIGO	RIESGO DE INCUMPLIMIENTO

RI01	No contar con el apoyo de las altas autoridades
RI02	Insuficientes recursos(humanos, equipos, espacio físico, etc.) para trabajar en la implementación
RI03	No contar con una cultura de riesgos en la institución
RI04	los responsables de TI no cuentan con el suficiente apoyo de las altas autoridades para realizar la gestión
RI05	No se cuenta con políticas institucionales para la gestión de TI
CODIGO	RIESGO EN LA GESTIÓN DE PROVEEDORES
RP1	Contratos no alineados a niveles de servicio (SLA)
CODIGO	RIESGO EN LA GESTIÓN DE LA INFORMACIÓN
RG01	Conformación inadecuada de contraseñas (insegura, débiles)
RG02	Uso compartido de contraseñas por parte de usuarios
RG03	Robo o pérdida de información por controles inadecuados
RG04	Capacitación inadecuada a los usuarios del sistema en la forma de administrar los recursos asignados
RG05	Confidencialidad de la información comprometida
RG06	Privacidad de la información comprometida
RG07	Integridad de la información comprometida por usuarios internos
RG08	Clasificación inadecuada de la información
RG09	Etiquetado inadecuado de la información

Fuente: Empresa Sitec Seguridad

Equipo Físico E Infraestructura

Ilustración 15- Ingreso cuarto IT



Fuente: Cuarto de IT de la empresa Sitec Seguridad

Ingreso al cuarto de IT presenta deficiencias en cuanto a seguridad, ya que no se cuenta con un sistema adecuado de control de entradas como lo es una bitácora de registro, no existen políticas claras que regulen el acceso a este espacio, lo que aumenta el riesgo de situaciones no autorizadas o peligrosas.

Ilustración 16- AP Aruba

SSID:	SItec Networks
Protocol:	Wi-Fi 4 (802.11n)
Security type:	WPA2-Personal

Fuente: AP de acceso wifi de la empresa Sitec Seguridad

Se observa un AP en área administrativa, realizando una revisión se encuentra que la configuración de la red es básica, ya que no se ha implementado ninguna VLAN ni restricciones adicionales más allá de una contraseña WPA2-Personal. Esta falta de segmentación y control aumenta la vulnerabilidad de la red, ya que no se aplican medidas de seguridad adicionales para proteger los diferentes segmentos o limitar el acceso a usuarios no autorizados.

Ilustración 17 -AP Ubiquiti

SSID:	SItec Networks
Protocol:	Wi-Fi 4 (802.11n)
Security type:	WPA2-Personal

Fuente: AP de acceso wifi de la Sitec Seguridad

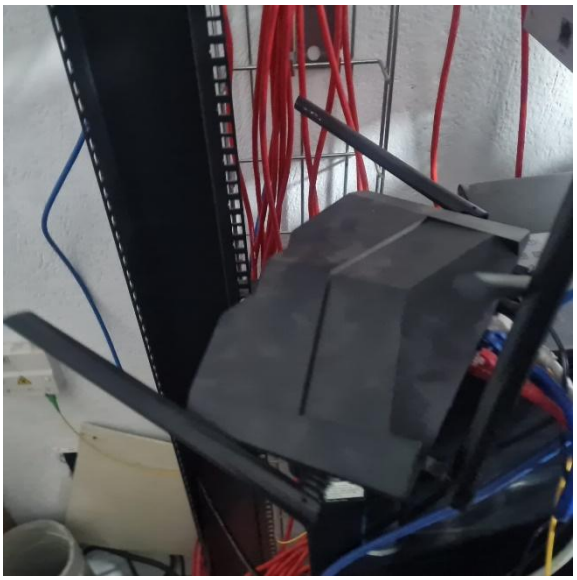
Se observa un AP en área de recepción, realizando una revisión se encuentra que la configuración de la red es básica, ya que no se ha implementado ninguna VLAN ni restricciones adicionales más allá de una contraseña WPA2-Personal, al igual que el del área administrativa esta falta de segmentación y control aumenta la vulnerabilidad de la red, ya que no se aplican medidas de seguridad adicionales para proteger los diferentes segmentos o limitar el acceso a usuarios no autorizados, adicionalmente el mismo no está colocado correctamente dejando la posibilidad de conectarse al punto de red de manera directa.

Ilustración 18- Módem de internet

Fuente: Módem de proveedor de servicios de la empresa Sitec Seguridad

Se cuenta con un módem del proveedor de servicios, el mismo esta segmentado con protección de puertos de tal manera que solo el equipo especifico puede estar conectado a el mismo, ofreciendo cierto nivel de seguridad en el extremo de internet.

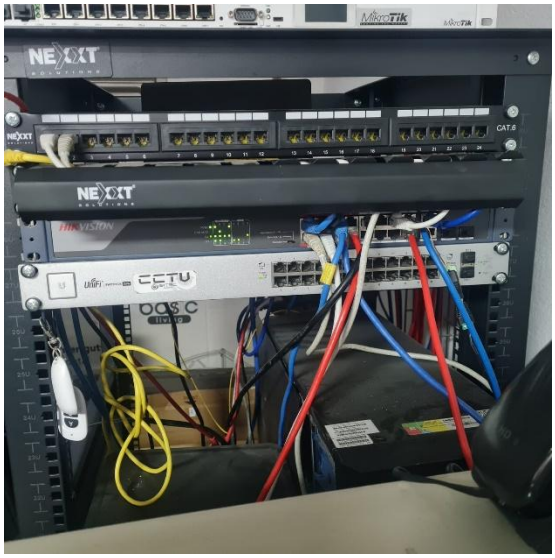
Ilustración 19- Router DCHP



Fuente: Router para direccionamiento DHCP de la empresa Sitec Seguridad

Se cuenta con un router para la asignación de DHCP de la red, posee configuración básica sin oportunidad de crear VLAN, sin ningún de segmentación de red de datos, wifi o usuarios, todos bajo una misma red plana. Esta falta de segmentación y control al igual que los "AP" aumenta la vulnerabilidad de la red, ya que no se aplican medidas de seguridad adicionales para proteger los diferentes segmentos o limitar el acceso a usuarios no autorizados.

Ilustración 20- Switch

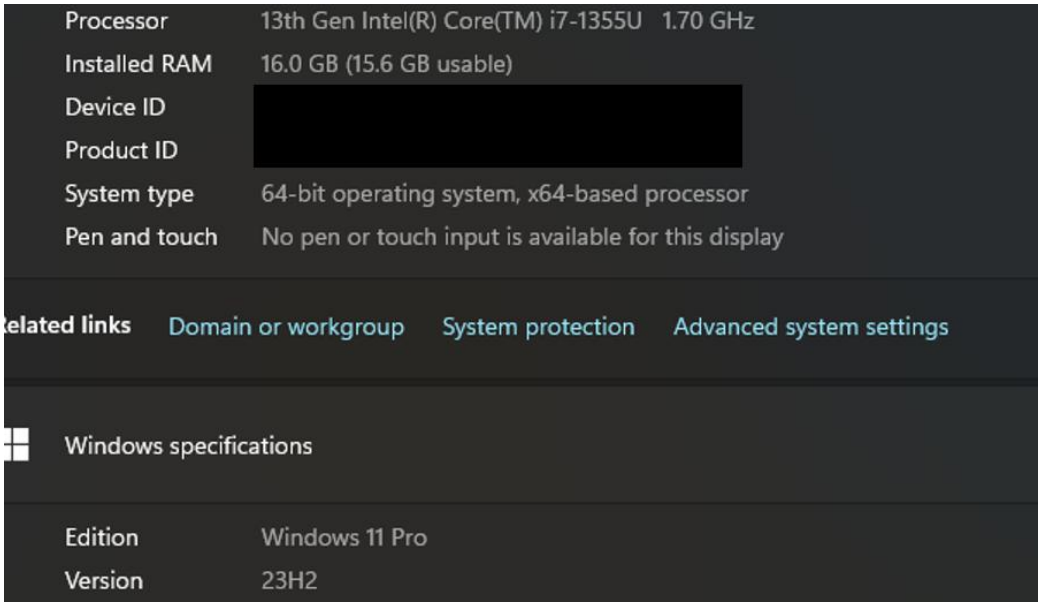


Fuente: Switch de red de la empresa Sitec Seguridad

Poseen un Switch apagado o sin uso y otro de un fabricante de CCTV, el cual es básico, al ser un equipo capa 2 no permite crear VLAN, no permite controlar puertos o ser asignados a una MAC en específico, por lo que no existe ningún tipo de restricción a nivel de puertos ni seguridad en los mismos, siendo uno de los equipos más vulnerables.

4 computadoras con las siguientes características:

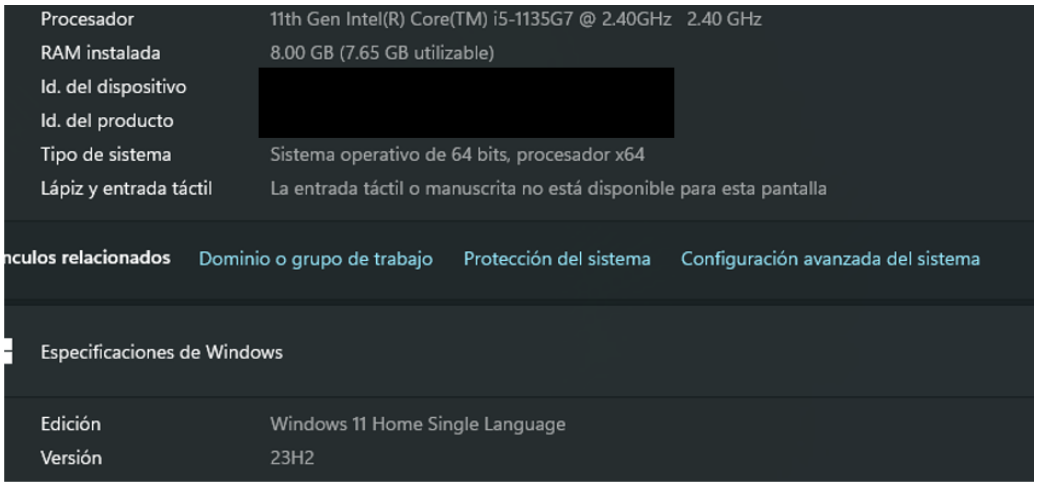
Ilustración 21 - Características computadores 1



Fuente: Computadores de la empresa Sitec Seguridad

2 computadora con las siguientes características:

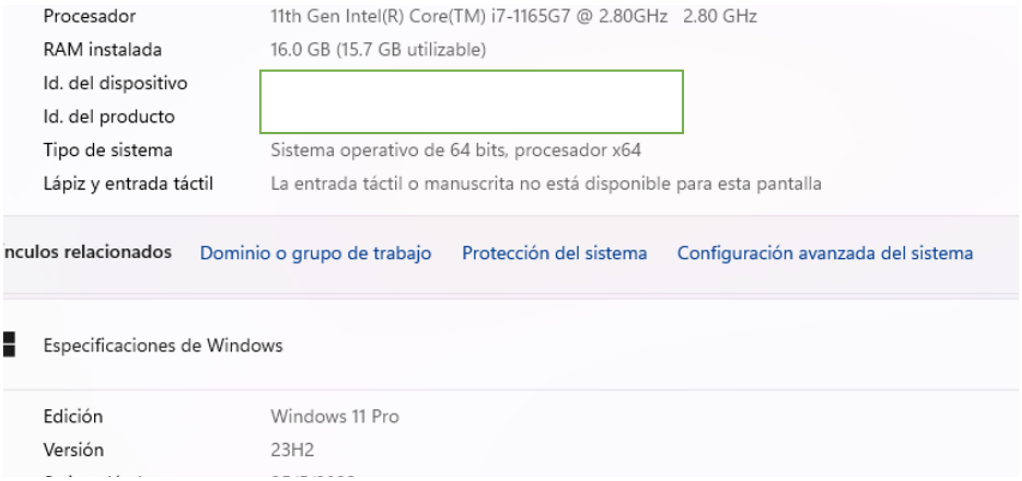
Ilustración 22- Características computadores 2



Fuente: Computadores de la empresa Sitec Seguridad

2 computadora con las siguientes características:

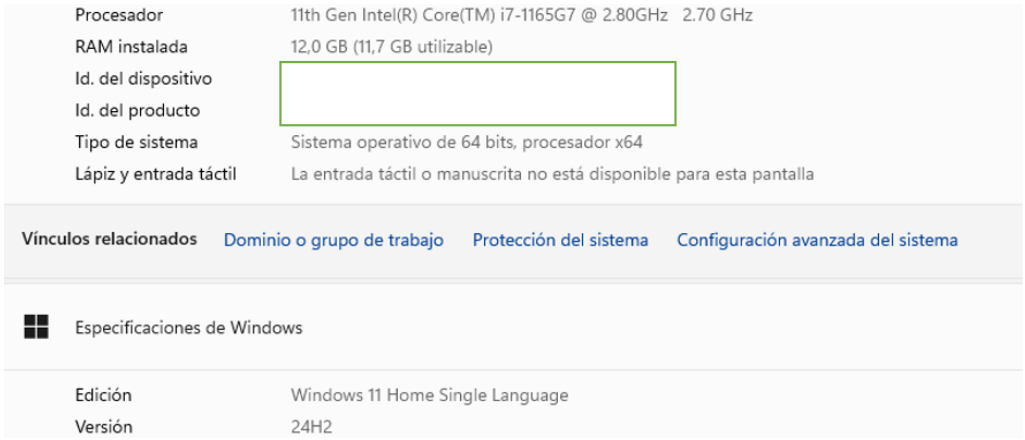
Ilustración 23- Características computadores 3



Fuente: Computadores de la empresa Sitec Seguridad

2 computadoras con las siguientes características:

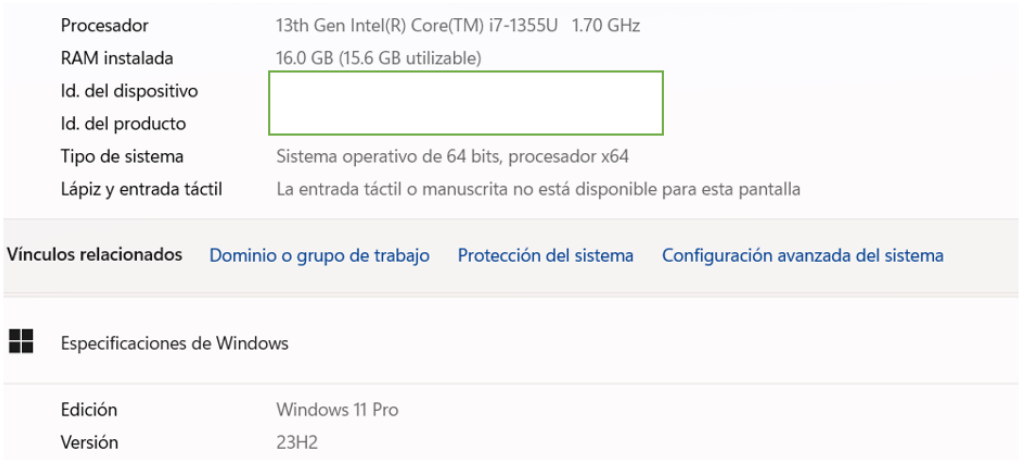
Ilustración 24- Características computadores 4



Fuente: Computadores de la empresa Sitec Seguridad

2 computadora con las siguientes características:

Ilustración 25- Características computadores 5



Fuente: Computadores de la empresa Sitec Seguridad

Tabla 7 - Comparación de computadoras

Cantidad	CPU	Sistema	RAM	Tipo sistema	Edición	Versión	Almacenamiento
4	13th	64 bits	16.0 GB	Windows	11 Pro	23H2	SSD
2	11th	64 bits	16.0 GB	Windows	11 Home	23H2	SSD
2	11th	64 bits	16.0 GB	Windows	11 Pro	23H2	SSD
2	11th	64 bits	16.0 GB	Windows	11 Home	24H2	SSD
3	Core i7 - 13th, 1.7 GHz	64 bits	16.0 GB	Windows	11 Pro	23H2	SSD

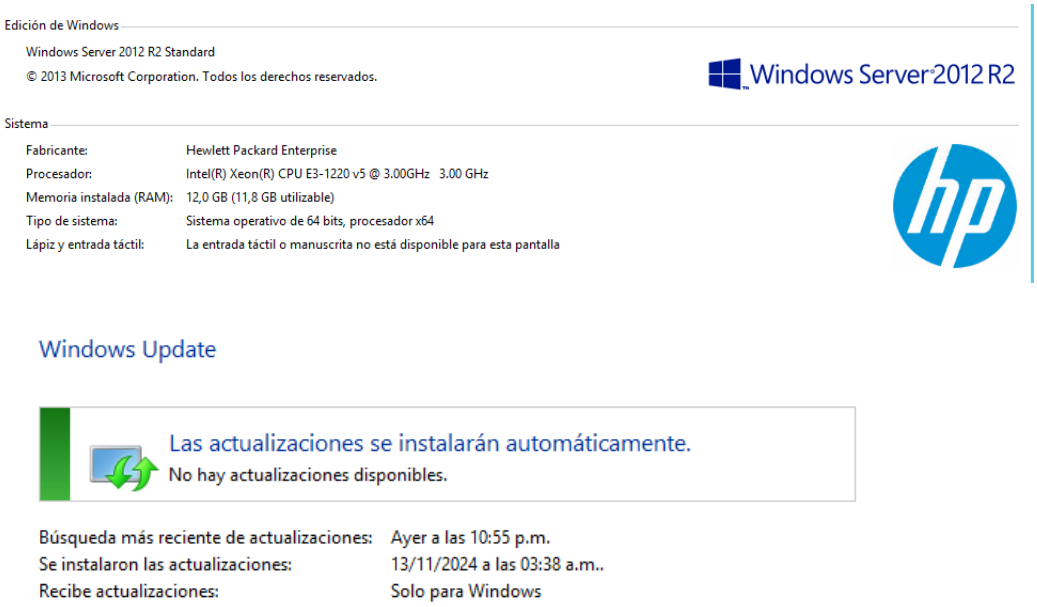
Fuente: Computadores de la empresa Sitec Seguridad

Las distintas computadoras están dentro de las generaciones 11th y 13th con sistema operativos Windows 11, con lo cual se puede obtener respaldo del fabricante Microsoft en actualizaciones, parches de seguridad y cualquier otro elemento que ofrezca seguridad a las mismas durante el 2025 y a la red en la que se encuentren.

Ilustración 26- Servidor de datos

Fuente: Servidor de datos de la Sitec Seguridad

Ilustración 27- Sistema operativo servidor



Fuente: características servidor de la empresa Sitec Seguridad

Se cuenta con un servidor de datos Server 2012 R2, como recomendaciones para detalles de actualizaciones, en equipos (Microsoft, 2023) nos indica lo siguiente:" Finaliza el soporte para Windows Server 2012 y 2012 R2.

La finalización del soporte de Windows Server 2012 y Windows Server 2012 R2 se producirá el 10 de octubre de 2023. Después de esta fecha, estos productos ya no recibirán actualizaciones de seguridad, actualizaciones que no son de seguridad, correcciones de errores, soporte técnico o actualizaciones de contenido técnico en línea. Si no puede actualizar a la siguiente versión, deberá usar Actualizaciones de seguridad extendidas (ESU) durante un máximo de tres años. Las ESU están disponibles de forma gratuita en Azure o deben adquirirse para implementaciones locales". Dentro de las recomendaciones brindadas por Microsoft están:

1. Migre a Azure y ejecute de forma segura con hasta tres años de actualizaciones de seguridad extendidas gratuitas
2. Actualización local a Windows Server 2022
3. Implementación de actualizaciones de seguridad extendidas en las instalaciones

1 Servidor de telefonía LINUX Server HP

Ilustración 28- Servidor de telefonía

Fuente: Características del servidor de telefonía de la empresa Sitec Seguridad

Diagnóstico De Percepción

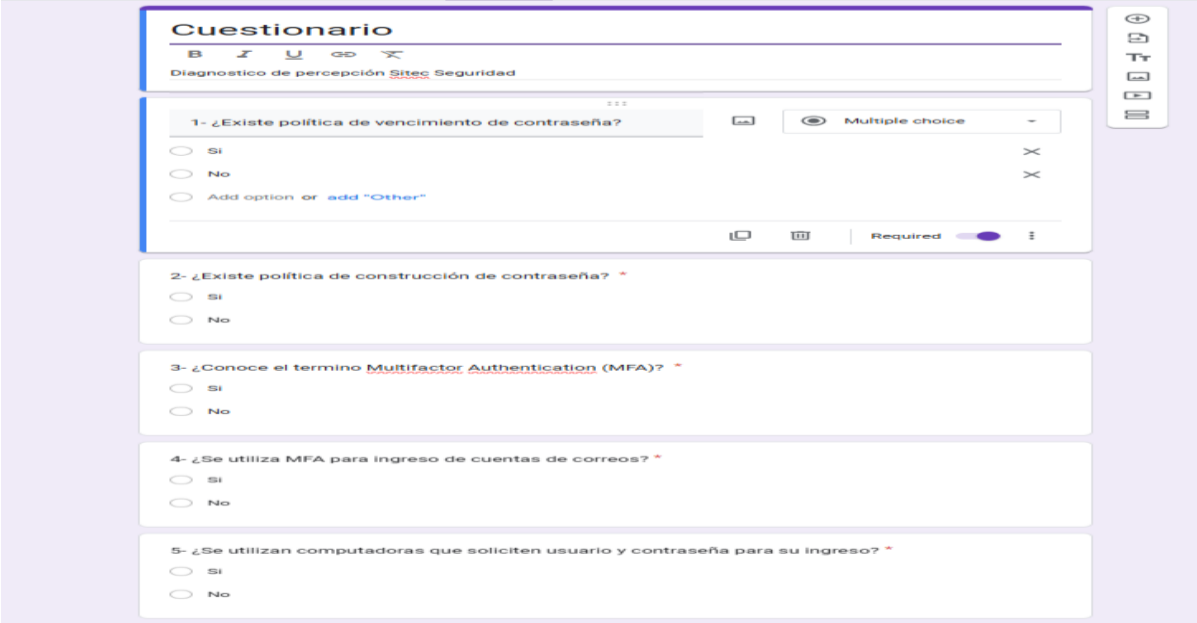
Durante el proceso de desarrollo de los diagnósticos a realizar a la empresa SITEC Seguridad durante este capítulo se realizó un análisis cuidadoso para garantizar que el diagnóstico de percepción reflejado en la encuesta está debidamente alineado tanto con la propuesta teórica como con los objetivos del proyecto y la gestión de estos.

La construcción de los ítems se ha basado en los conceptos clave abordados durante el capítulo 2 del marco teórico, permitiendo así explorar de forma coherente las dimensiones planteadas desde una perspectiva académica y contextual.

De igual forma cada una de las preguntas ha sido diseñada para aportar evidencia que permita responder a los objetivos específicos del proyecto, asegurando que los datos recolectados contribuyan directamente al análisis, la toma de decisiones y la propuesta de soluciones dentro del proceso de gestión con lo cual se asegura que la encuesta este alineada de manera pertinente y estratégica con el enfoque teórico adoptado y con la planificación general del proyecto.

Se desarrolló un formulario en relación a políticas de gestión de la seguridad de la información que van de la mano con el marco de gestión COBIT2019 para conocer el estado actual por parte de los colaboradores de la empresa Sitec Seguridad.

Ilustración 29- Cuestionario percepción



Fuente: Elaboración propia

Ilustración 30- Pregunta 1

Fuente: Cuestionario

Como se muestra en la gráfica anterior alrededor del 30% de la población desconoce si existe una política de vencimiento de contraseña dentro de la empresa Sitec Seguridad, por lo cual es importante el desarrollo de una política de cultura de seguridad de la información dentro de la empresa, donde se permita concientizar a los colaboradores de este protocolo tan importante, la propuesta incluye el desarrollo de una política de vencimiento de contraseña para ser expuesta a la empresa Sitec Seguridad.

Ilustración 31- Pregunta 2

Fuente: Cuestionario

El grafico anterior muestra que alrededor de un 18% de los colaboradores no conocen la existencia de una política de construcción de contraseña, lo cual es una brecha de seguridad para la organización debido a que muchas de las contraseñas que utilizan los colaboradores de Sitec Seguridad son vulnerables a ciberataques o ataques informáticos.

(Picheta, 2019) por su parte nos menciona: “Las 10 contraseñas más comunes fueron:

123456

123456789

qwerty

password

111111

12345678

abc123

1234567

password1

12345

El procedimiento de construcción de contraseñas que se incluye en el capítulo 5 del proyecto, es de gran valor e importancia pues concientizara a los colaboradores la importancia de un protocolo de construcción de contraseñas para mantener un ambiente seguro.

Ilustración 32 - Ataque fuerza bruta

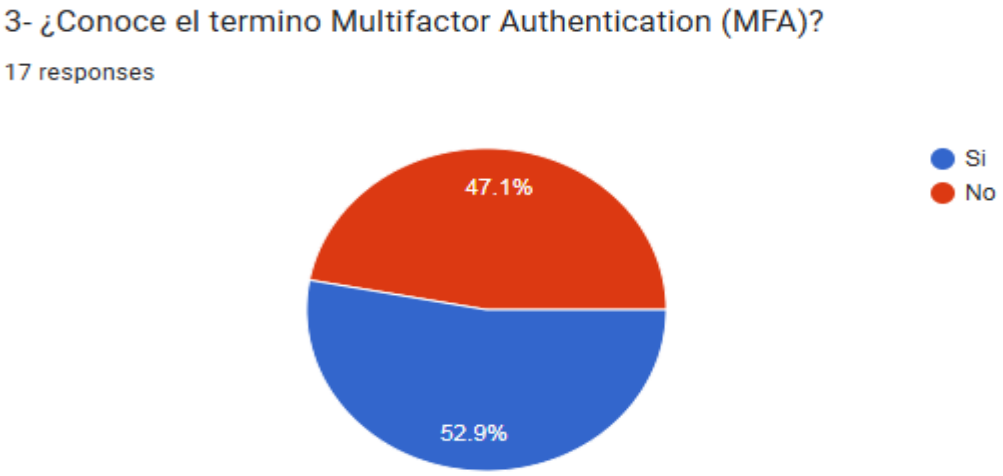
EL TIEMPO QUE CUESTA UN HACKER PARA ROBAR TU CONTRASEÑA A TRAVÉS DE UN ATAQUE DE FUERZA BRUTA EN 2024

12 x RTX 4090 | bcrypt

Número de caracteres	Sólo numeros	Sólo minúsculas	Mayúsculas y minúsculas	Numeros, mayúsculas y minúsculas	Numeros, mayúsculas y minúsculas, y simbolos
4	Instantáneo	Instantáneo	3 segundos	6 segundos	9 segundos
5	Instantáneo	4 segundos	2 minutos	6 minutos	10 minutos
6	Instantáneo	2 minutos	2 horas	6 horas	12 horas
7	4 segundos	50 minutos	4 días	2 semanas	1 mes
8	37 segundos	22 horas	8 meses	3 años	7 años
9	6 minutos	3 semanas	33 años	161 años	479 años
10	1 hora	2 años	1000 años	9 mil años	33 mil años
11	10 horas	44 años	89 mil años	618 mil años	2 millón años
12	4 días	1 mil años	4 millón años	38 millón años	164 millón años
13	1 mes	29 mil años	241 millón años	2 mil millones años	11 mil millones años
14	1 año	766 mil años	12 mil millones años	147 mil millones años	805 mil millones años
15	12 años	19 millón años	652 mil millones años	9 billón años	56 billón años
16	119 años	517 millón años	33 billón años	566 billón años	3 mil billones años
17	1000 años	13 mil millones años	1 mil billones años	35 mil billones años	276 mil billones años
18	11 mil años	350 mil millones años	91 mil billones años	2 trillón años	19 trillón años

Fuente: (Neskey, 2024)

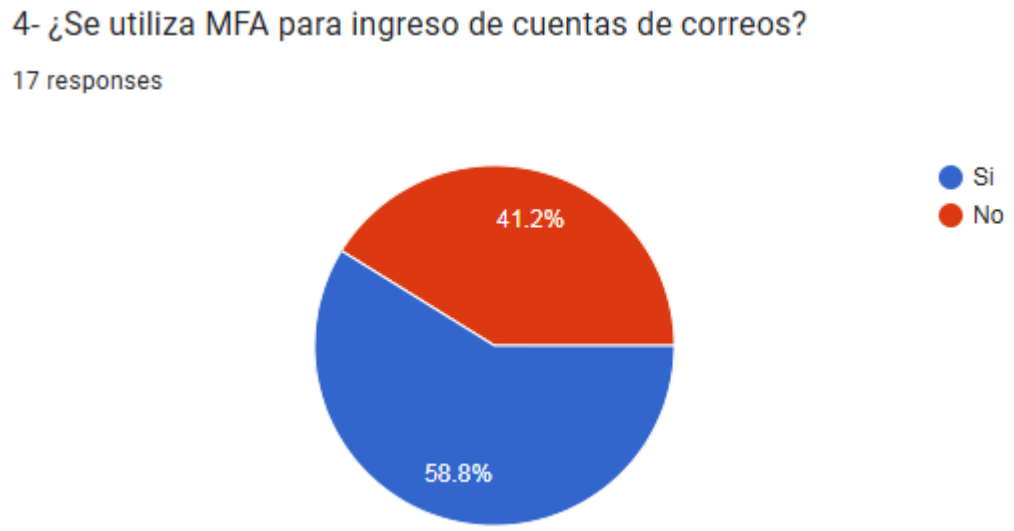
Ilustración 33- Pregunta 3



Fuente: Cuestionario

Como refleja la pregunta 3, el 47.1% de los colaboradores desconoce del termino MFA, lo cual deja en evidencia la falta de implementación correcta y el uso adecuado del mismo dentro de la organización, de ahí la importancia de culturizar a los mismos con una propuesta que se desarrolla en el capítulo 5 de este trabajo.

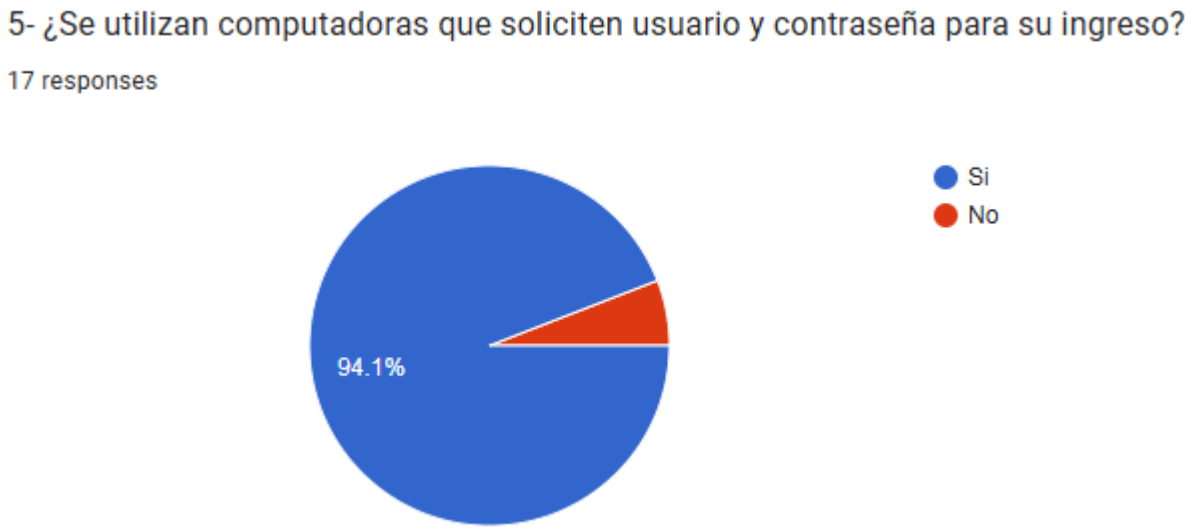
Ilustración 34- Pregunta 4



Fuente: Cuestionario

El 41% de los colaboradores de la empresa no utilizan un MFA lo cual los hace vulnerables a un ataque exponencial de fuerza bruta, como se detalló en preguntas anteriores, la propuesta plantea protocolos de Multifactor de Autenticación para la empresa Sitec Seguridad.

Ilustración 35- Pregunta 5



Fuente: Cuestionario

El 5.1% que equivale a 1 de los colaboradores de la empresa dice no utilizar una computadora que solicite usuario y contraseña lo cual los hace vulnerables, exponiendo información sensible de la compañía, la propuesta plantea políticas de creación y uso de contraseñas para la empresa Sitec Seguridad.

Ilustración 36- Pregunta 6

Fuente: Cuestionario

Como se observa en el grafico cerca del 18% de los colaboradores de la empresa comparten su usuario y contraseña con otros compañeros o personas, mostrando una vulnerabilidad exponencial a la información y equipos de la empresa, la propuesta plantea culturización a los colaboradores sobre el manejo de contraseñas en la empresa Sitec Seguridad.

Ilustración 37- Pregunta 7

Fuente: Cuestionario

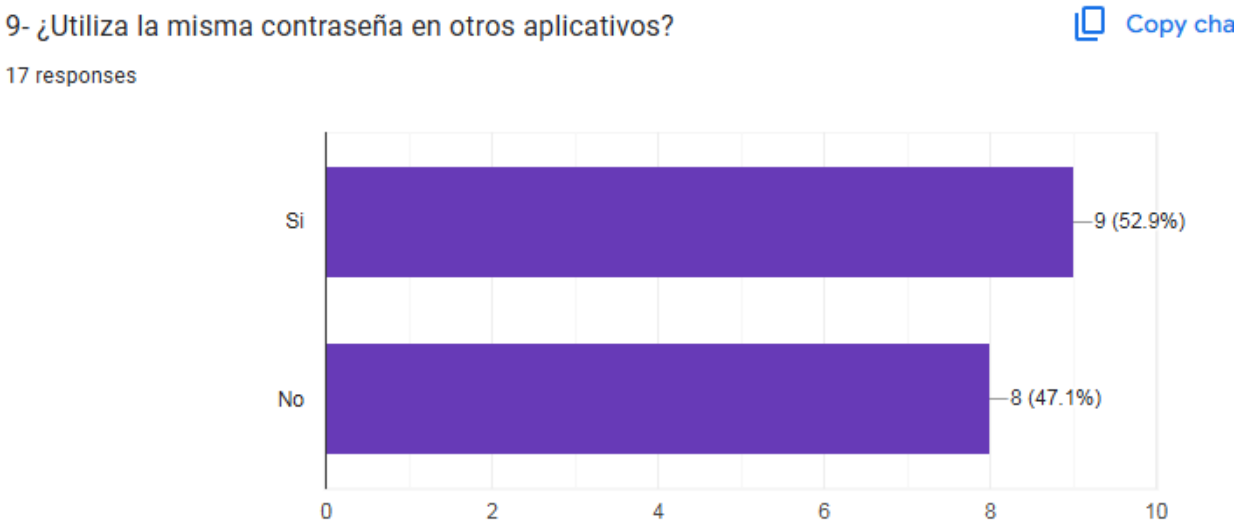
El 11.8 % de los colaboradores o su equivalente a 2 personas de la empresa indican tener la contraseña visible, dejando una brecha de seguridad y vulnerabilidad de los equipos e información dentro de los mismos, la propuesta plantea políticas desde la creación hasta el manejo de contraseñas para la empresa Sitec Seguridad.

Ilustración 38- Pregunta 8

Fuente: Cuestionario

La grafica anterior muestra que el 41.2 % de los colaboradores de la empresa utilizan el mismo usuario y contraseña en más de 1 equipo, dejando una brecha de seguridad desde el punto de vista que si la misma es descifrada ponen en riesgo otros equipos o sistemas de la información dentro de la empresa Sitec Seguridad.

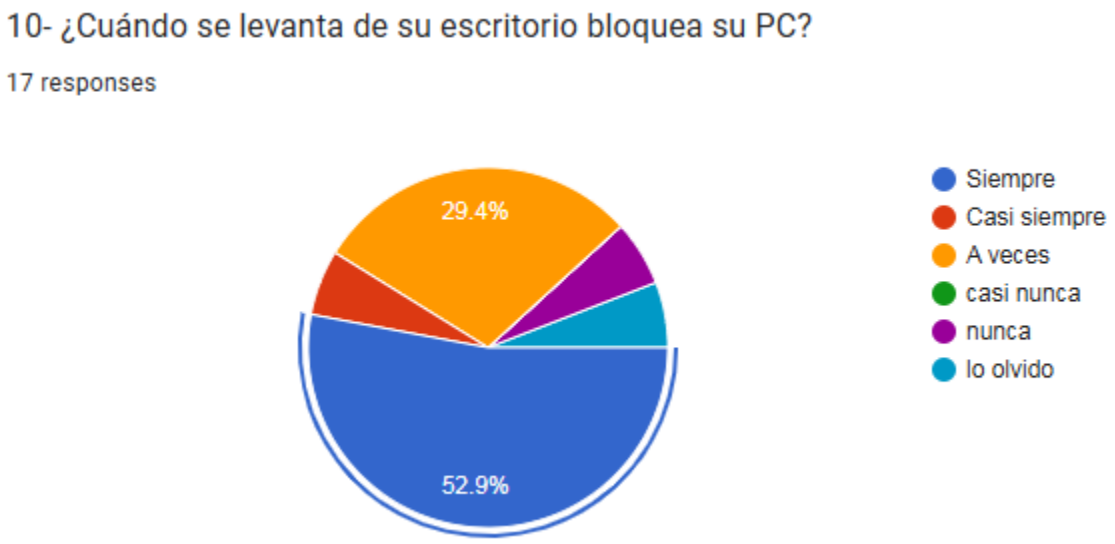
Ilustración 39- Pregunta 9



Fuente: Cuestionario

Como se muestra en la gráfica 52.9 % de los colaboradores de la empresa utilizan el mismo usuario y contraseña en más de 1 equipo, dejando una vulnerabilidad importante de seguridad desde el punto de vista que si la misma es descifrada ponen en riesgo sistemas y la información dentro de la empresa Sitec Seguridad, el capítulo 5 presenta una propuesta del uso adecuado de las contraseñas.

Ilustración 40- Pregunta 10



Fuente: Cuestionario

En el grafico anterior se observa que cerca del 47% de los colaboradores olvida al menos 1 vez bloquear el computador, lo que se convierte en una brecha de seguridad por la información sensible que se maneja en cada una de los dispositivos, dentro de la propuesta del capítulo 5 se desarrollarán campañas de concientización, de cultura de manejo de la información para los colaboradores de la empresa Sitec Seguridad

Ilustración 41- Pregunta 11

Fuente: Cuestionario

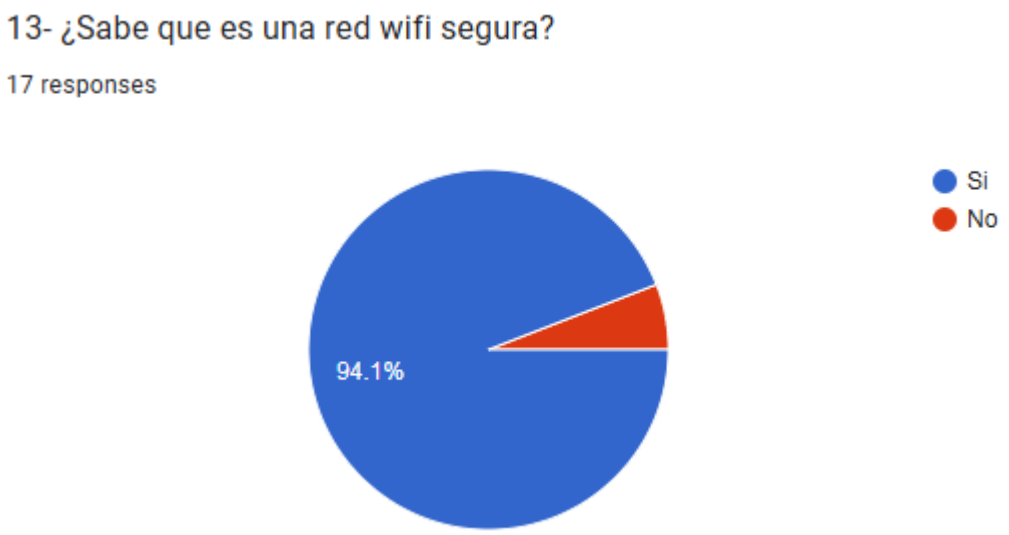
Cerca del 24 % de los colaboradores de la empresa desconoce si existe una política del manejo de la información, por lo cual se va estar dando información sensible de la compañía a personas no autorizadas y de la manera incorrecta, en el capítulo siguiente se reforzará la misma y se aclarará a los colaboradores sobre la misma y manera correcta de hacerla efectiva dentro y fuera de la empresa Sitec Seguridad.

Ilustración 42- Pregunta 12

Fuente: Cuestionario

Al no conocer o tener claridad sobre una política de manejo de la información los colaboradores desconoces con quien, como y cual información dar y la gráfica indica que el 23.5 % de los colaboradores de la empresa es consiente que brinda información sensible a otras personas, poniendo en riesgo toda la operativa de la empresa.

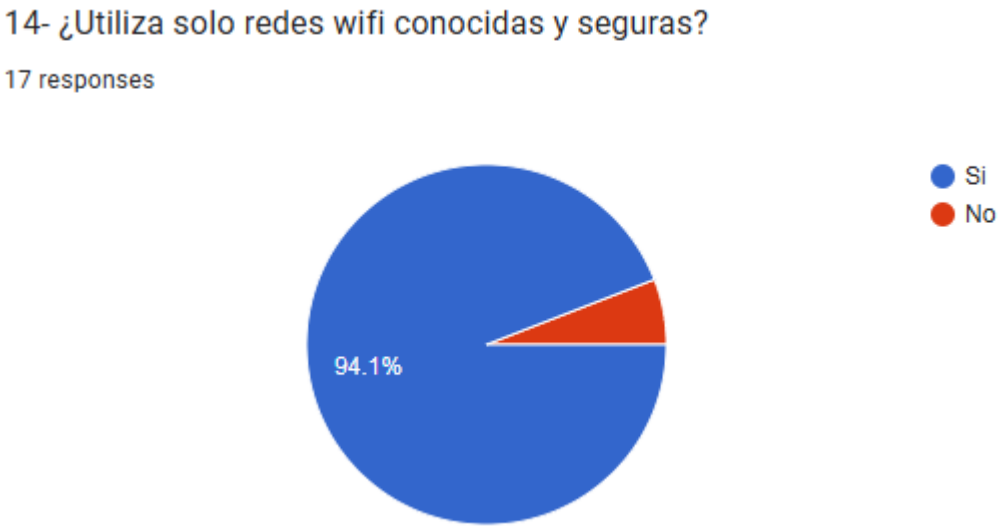
Ilustración 43- Pregunta 13



Fuente: Cuestionario

Una persona o su equivalente al 5.9 % de los colaboradores de la empresa no sabe que es una red segura, con lo cual deja una vulnerabilidad de seguridad importante conectándose a equipos no autorizados o seguros, dejando la información de su equipo exponencialmente insegura y con posibilidad de ser tomada por otras personas ajenas a la empresa, dentro de la propuesta se plantean políticas y protocolos de conexión seguros con el fin de hacer conciencia y una correcta aplicación de los mismos dentro y fuera de la empresa Sitec Seguridad.

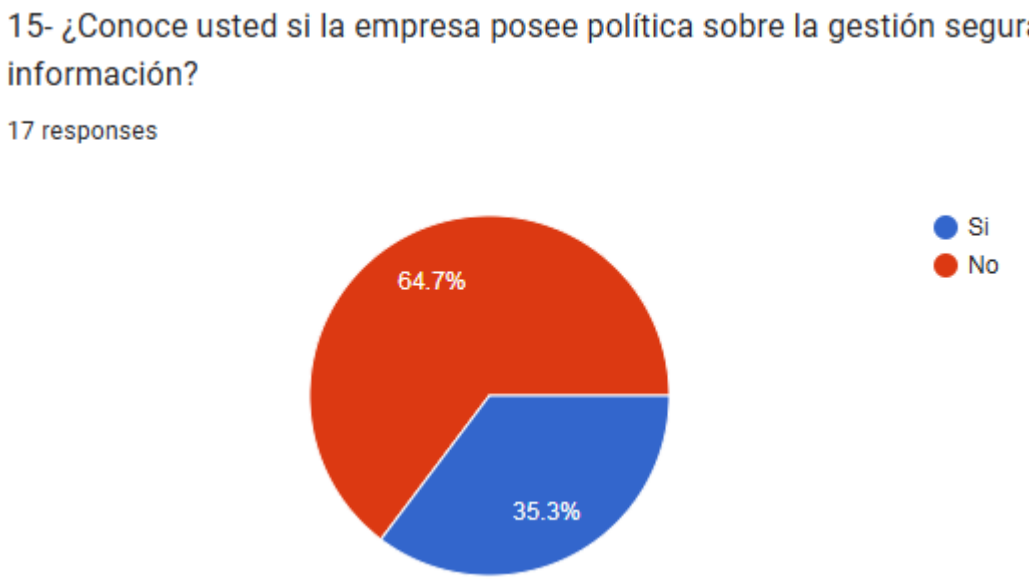
Ilustración 44- Pregunta 14



Fuente: Cuestionario

La grafica anterior indica que el 5.9 % de los colaboradores de la empresa utilizan cualquier red wifi, dejando una brecha de seguridad grave desde el punto de vista que la maquina o dispositivo utilizado es sensible a posibles ciberataques poniendo en riesgo otros equipos o sistemas de la información dentro de la empresa Sitec Seguridad.

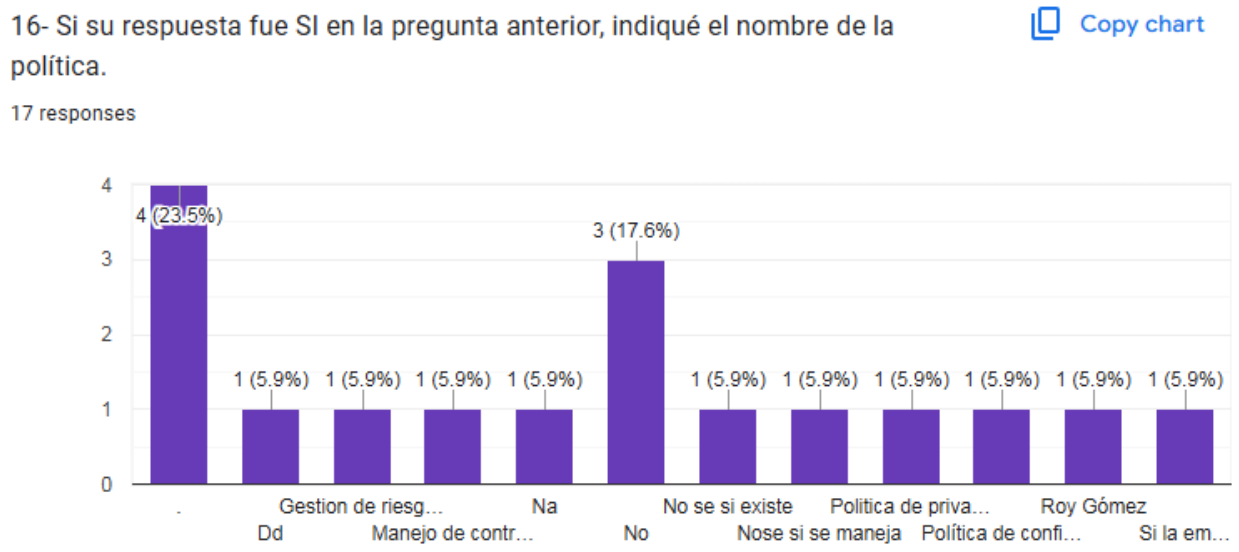
Ilustración 45- Pregunta 15



Fuente: Cuestionario

Cerca del 65% de los colaboradores de Sitec Seguridad no conocen de la existencia de una política sobre la gestión segura de la información, además al realizar las consultas a las personas que dicen conocer la política no detallan correctamente el nombre de la misma, con lo que se evidencia desconocimiento total a esto en cuanto a política gestión segura de la información.

Ilustración 46- Pregunta 16



Fuente: Cuestionario

La grafica anterior evidencia como se menciona anteriormente un desconocimiento total de la política y con ello una aplicación incorrecta de la mismas dentro de la organización, de ahí que se desarrolla un plan de revisión, capacitación y puesta en práctica de la misma con el personal de la empresa Sitec Seguridad durante el capítulo 5.

Durante este capítulo se brindaron los diagnósticos de la investigación, se proporcionaron las falencias y recomendaciones, así como la metodología de la investigación del proyecto, este tuvo como objetivo brindar un enfoque claro de la situación actual de la empresa Sitec Seguridad, tanto en el ámbito teórico como práctico de tal manera que garantiza que el estudio se realizó de una manera ordenada y eficaz.

El primer diagnóstico realizado desde un enfoque administrativo se encargó de verificar los procedimientos, protocolos y prácticas implementadas por la empresa en relación con la gestión de las Tecnologías de la Información (TI). Este diagnóstico incluyó una revisión de los

documentos y manuales existentes, así como una evaluación del cumplimiento de las normativas y directrices que rigen la gestión de TI dentro de la organización, este análisis permite identificar las brechas o deficiencias presentes en los procesos actuales, lo que determino las áreas que requieren ajustes, el proceso proporciono resultados significativos, tales como la identificación de la falta de procedimientos adecuados, la necesidad de mejorar o ajustar los existentes, y la importancia de actualizar al personal sobre la correcta implementación y seguimiento de los procedimientos vigentes, este enfoque no solo facilita la mejora continua, sino también garantiza una gestión más eficiente de las TI en la empresa Sitec Seguridad.

El segundo diagnóstico se enfocó en los activos tecnológicos de la empresa, se consideró tanto el software como el hardware utilizado para la gestión y almacenamiento de la información, se realizó un inventario de los activos tecnológicos existentes, evaluando su estado, eficiencia y capacidad, se analizó la infraestructura física, que incluyó los servidores, centros de datos, topologías de red y la planta física, que son componentes esenciales en la gestión de la información.

El tercer y último diagnóstico brindó la percepción de los colaboradores de la empresa, a través de entrevistas y cuestionarios diseñados para este fin, adicionalmente se recopilaron opiniones sobre los procesos y prácticas actuales en la gestión de la información, dichas preguntas del cuestionario estaban dirigidas a evaluar la percepción y efectividad de las herramientas o sistemas utilizados, así como a conocer el grado de conocimiento y cumplimiento de los protocolos establecidos en la empresa por parte de los colaboradores, lo que permitió identificar las áreas de mejora en las que los colaboradores interactúan directamente con las TI en su trabajo cotidiano.

CAPÍTULO 5

PROPUESTA

En desarrollo de este capítulo se presentará la propuesta para la implementación de protocolos y buenas prácticas orientadas a los procesos establecidos en el Marco Normativo de Gobernanza y Gestión del Departamento de TI de Sitec Seguridad (Sistemas Integrados de Seguridad S.A.), con base en las normas ISO/IEC27001:2022 Sistema de Gestión de Seguridad de la Información y el ISO/IEC 27002:2022 Controles de Seguridad de la Información y Ciberseguridad aplicados en el Marco de Referencia Cobit 2019. Se desarrollarán propuestas para la implementación de políticas, las cuales tienen como objetivo fortalecer la gestión y seguridad de los sistemas de información de Sitec Seguridad, alineándolos con estándares internacionales y mejores prácticas del sector, garantizando la confidencialidad, integridad y disponibilidad de los datos.

La implementación se logrará mediante el desarrollo de un Manual de gestión de seguridad de la información, el cual incluirá los controles necesarios para cumplir con las NORMAS ISO 27001 e ISO 27002. Estas normativas, incluidas en el Marco de Referencia COBIT 2019 en sus apartados relacionados con Seguridad y Ciberseguridad, asegurando así una gestión adecuada de los riesgos y una protección eficaz de los activos de información de la organización.

Se puede decir que el sistema de gestión de seguridad de la información (SGSI) está fundamentado en 2 parámetros: identificación y análisis de amenazas para la empresa Sitec Seguridad, a partir de este punto se establece una evaluación y se planifica el tratamiento que se dará a los riesgos encontrados.

La constante amenaza o riesgo de pérdida de información, datos comprometidos, daño de sistemas está presente día a día, a través del recurso humano como el principal actor en afectar la

información y activos de la empresa Sitec Seguridad, está afectación se puede dar por desconocimiento en temas de seguridad, así como por una clara participación y conocimiento de causa del hecho realizado, de ahí que el ISO 27001:2022 propicia una cultura de seguridad de la información dentro de la empresa, proporcionando procedimientos, procesos y controles aplicados por medio de COBIT 2019.

Se utilizarán los siguientes objetivos los cuales están relacionados con seguridad y ciberseguridad, como lo son:

- APO13: Gestión de la seguridad

Este APO basado en las políticas y usando buenas prácticas de COBIT 2019 para la implementación de un sistema de gestión de seguridad de información (SGSI) y se le aplicarán los siguientes controles:

1. Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).
2. Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.
3. Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).

Tabla 8 - Matriz APO13 Sitec Seguridad

Regresar a Inicio

Matriz Guía para la Implementación de Buenas prácticas Basadas en Cobit 2019
Ficha Implementación de Objetivo de Gobierno/Gestión

Sitec Sistemas Integrados de Seguridad S.A.

Dominio: Alinear, Planificar y Organizar
Objetivo de Gestión: APO13—Gestionar la seguridad
Proceso relacionado del Marco Normativo: Seguridad y Ciberseguridad
Riesgos Asociados:

Prioridad de Implementación: Etapa 1

Implementable	Porcentaje Avance	Fecha Conclusión Implementación
		5/3/2027

Práctica de Gobierno (gestión): 01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).

Indicadores Asociados: a. Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance.	Sí	5/3/2025	En Proceso		Jorge Sancho		Docuementos existente de la empresa, COBIT 2019, ISO 27001, ISO 27002	Se obtiene el aporte de gerencia general y gerencia de tecnologia para el desarrollo de este
2 Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa.	Sí	5/3/2025	En Proceso		Christian Sancho		Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se obtiene el aporte de gerencia general y gerencia de tecnologia.
3. Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad.	Sí	5/3/2025	En Proceso		Christian Sancho		Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se debe contar con el apoyo de gerencia general y gerencia de tecnologia de la informacion
4 Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI.	Sí	5/3/2025	En Proceso		Jorge Sancho		Documentos existentes de la empresa, COBIT 2019, ISO 27001, ISO 27002	Se obtiene por la gerencia la indicación de desarrollar los 20 controles de seguridad más necesarios
5 Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.	Sí	5/3/2025	En Proceso		Christian Sancho		Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de preparar y mantener recae sobre el funcionario asignado al puesto de gerencia de tecnología de la información.
6. Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información.	Sí	5/3/2025	En Proceso		Christian Sancho		Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de definir y comunicar los roles recae sobre el funcionario asignado al puesto de gerencia de tecnología de la
7. Comunicar la estrategia de SGSI.	Sí	5/3/2025	En Proceso		Christian Sancho		Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de comunicar la estrategia recae sobre el funcionario asignado al puesto de gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.

Indicadores Asociados: a. Porcentaje de simulaciones de escenarios de riesgo de seguridad exitosas.
b. Número de empleados que han completado con éxito una formación de concienciación sobre seguridad de la información

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	Se desarrollan 20 controles de seguridad, los 20 controles mas necesarios
2 Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad.	Sí	5/3/2025	En Proceso		Christian Sancho / Iriam Hernandez	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de inventario recae sobre la gerencia de tecnología de la información.
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad, apoyadas por casos de negocio apropiados que incluyan consideraciones de financiación y asignación de roles y responsabilidades.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	Se desarrollan 20 controles de seguridad, los 20 controles mas necesarios
4 Proporcionar aportes para el diseño y desarrollo de prácticas y soluciones de gestión, seleccionadas en el plan de tratamiento de riesgos de seguridad de la información.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	Se desarrollan 20 controles de seguridad, los 20 controles mas necesarios
5 Implementar programas de formación y concienciación sobre seguridad de la información y privacidad.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	Se entrega una matriz de cursos gratuitos para la formación
6. Integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	Se recomienda dentro del proyecto dar capacitaciones almenos con frecuencia de cutrimestral o semestral
7. Definir cómo medir la eficacia de las prácticas de gestión seleccionadas. Especificar cómo deben usarse estas medidas para evaluar la eficacia para producir resultados comparables y reproducibles.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de medición de eficacia recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).

Indicadores Asociados:
a. Frecuencia de revisiones de seguridad programadas.
b. Número de hallazgos en revisiones de seguridad programadas regularmente.
c. Nivel de satisfacción de las partes interesadas con el plan de seguridad.
d. Número de incidentes relacionados con la seguridad causados por no adherirse adecuadamente al plan de seguridad

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	La responsabilidad recae sobre la gerencia de tecnología de la información.
2 Realizar auditorías de SGSI a intervalos planificados..	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	La responsabilidad recae sobre la gerencia de tecnología de la información.
3. Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	La responsabilidad recae sobre la gerencia de tecnología de la información.
4 Registrar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	La responsabilidad recae sobre la gerencia de tecnología de la información.
5 Hacer aportes para el mantenimiento de los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	COBIT 2019, ISO 27001, ISO 27002	La responsabilidad recae sobre la gerencia de tecnología de la información.

- DSS05: Gestión de los servicios de seguridad

Para este objetivo se utilizará las políticas y las buenas prácticas de COBIT2019 para la implementación de un sistema de gestión de seguridad de información (SGSI) y aplicando los siguientes controles:

1. Proteger contra software malicioso.
2. Gestionar la seguridad de la conectividad y de la red.
3. Gestionar la seguridad de EndPoint.
4. Gestionar la identidad del usuario y el acceso lógico.
5. Gestionar el acceso físico a los activos de IT.
6. Gestionar documentos sensibles y dispositivos de salida.
7. Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.

Tabla 9 - Matriz DSS05 Sitec Seguridad

Regresar a Inicio

Matriz Guía para la Implementación de Buenas prácticas Basadas en Cobit 2019
Ficha Implementación de Objetivo de Gobierno/Gestión

Sitec Sistemas Integrados de Seguridad S.A.

Dominio: Entregar, dar servicio y soporte

Objetivo de Gestión: DSS05 -Gestionar los servicios de seguridad

Proceso relacionado del Marco Normativo: Seguridad y Ciberseguridad

Riesgos Asociados:

Práctica de Gobierno (gestión): 01 - Proteger contra software malicioso.

Indicadores Asociados:
a. Número de ataques exitosos de software malicioso
b. Porcentaje de empleados que no pasan las pruebas de ataques maliciosos (p. ej., la prueba de correos electrónicos de phishing)

Prioridad de Implementación: Etapa 1

Implementable	Porcentaje Avance	Fecha Conclusión Implementación
		5/3/2027

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Instalar y activar herramientas de protección contra software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automáticamente o semiautomáticamente)	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se debe contar con el apoyo de gerencia general y gerencia de tecnologia de la informacion
2 Filtrar el tráfico de entrada, como el correo electrónico y las descargas, para protegerlo de información no solicitada (p.ej. spyware, correos electrónicos de phishing).	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad recae sobre la gerencia de tecnología de la información.
3 Comunicar acerca de concienciación sobre software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención. Impartir formación periódica sobre malware en el uso de correo electrónico e Internet. Formar a los usuarios para que no abran e informen sobre correos electrónicos sospechosos y no instalen software compartido o no aprobado.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de comunicar e impartir recae sobre la gerencia de tecnología de la información, se brinda una matriz de cursos gratuitos para la empresa.
4 Distribuir todo el software de protección centralmente (versión y parches) usando una configuración centralizada y la gestión de cambios de TI.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de distribuir el software recae sobre la gerencia de tecnología de la información.
5 Revisar y evaluar la información sobre nuevas amenazas potenciales (p. ej., revisión de los consejos de seguridad de productos y servicios de proveedores) de forma regular.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de revisar y evaluar recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 02 -Gestionar la seguridad de la conectividad y de la red.

Indicadores Asociados: a. Número de brechas del firewall

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Permitir que solo los dispositivos autorizados tengan acceso a la información corporativa y a la red de la empresa. Configurar estos dispositivos para forzar la introducción de contraseña.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad recae sobre la gerencia de tecnología de la información.
2 Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusos. Hacer cumplir las políticas adecuadas para controlar el tráfico entrante y saliente.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se debe contar con el apoyo de gerencia general y gerencia de tecnologia de la informacion
3 Aplicar protocolos de seguridad aprobados a las conexiones de red.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de aplicar protocolos recae sobre la gerencia de tecnología de la información.
4 Configurar el equipo de red de forma segura.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de configurar los equipos recae sobre la gerencia de tecnología de la información.
5 Encriptar la información en tránsito de acuerdo a su clasificación.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de encriptar la información recae sobre la gerencia de tecnología de la información.
6 Establecer y mantener una política para la seguridad de la conectividad con base en las evaluaciones de riesgo y los requisitos del negocio.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de establecer y mantener una politica recae sobre la gerencia de tecnología de la información y aprobada por la gerencia general.
7 Establecer mecanismos confiables para apoyar la transmisión y recepción segura de la información.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de mecanismos confiables recae sobre la gerencia de tecnología de la información.
8 Llevar a cabo pruebas de penetración periódicas para determinar la idoneidad de la protección de la red.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de realizar pruebas de penetración recae sobre la gerencia de tecnología de la información.
9 Llevar a cabo pruebas periódicas a la seguridad del sistema para determinar la idoneidad de la protección del sistema.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de realizar pruebas recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 03 -Gestionar la seguridad de endpoint.

Indicadores Asociados: a. Número de incidentes que involucran a dispositivos endpoint

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Configurar los sistemas operativos de forma segura.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de configurar los sistemas recae sobre la gerencia de tecnología de la información.
2 Implementar mecanismos de bloqueo de dispositivos.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de implementar mecanismos de bloqueo recae sobre la gerencia de tecnología de la información.
3 Gestionar el acceso y control remotos (p.ej. dispositivos móviles, teletrabajo)	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura,	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se desarrollan 20 controles de seguridad, los 20 controles mas necesarios
4 Gestionar la configuración de red de forma segura.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura,	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se desarrollan 20 controles de seguridad, los 20 controles mas necesarios
5 Implementar el filtrado de tráfico de red en dispositivos de punto final.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de realizar pruebas recae sobre la gerencia de tecnología de la información.
6 Proteger la integridad del sistema.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de realizar pruebas recae sobre la gerencia de tecnología de la información.
7 Proporcionar protección física a los dispositivos de punto final.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de realizar pruebas recae sobre la gerencia de tecnología de la información.
8 Eliminar de forma segura los dispositivos Endpoint	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura,	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se desarrollan 20 controles de seguridad, los 20 controles mas necesarios
9 Gestionar el acceso malicioso a través del correo electrónico y los navegadores web. Por ejemplo, bloquear determinados sitios web y desactivar los clics a enlaces para los smartphones.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de realizar pruebas recae sobre la gerencia de tecnología de la información.
10 Encriptar la información almacenada de acuerdo a su clasificación.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de realizar pruebas recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 04 -Gestionar la identidad del usuario y el acceso lógico.
Indicadores Asociados: a. Tiempo promedio entre el cambio y la actualización de cuentas

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Mantener los derechos de acceso de los usuarios de acuerdo con la función del negocio, los requisitos del proceso y las políticas de seguridad. Alinear la gestión de identidades y derechos de acceso con los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad-de-tener y necesidad-de-conocer	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se desarrollan 20 controles de seguridad, los 20 controles mas necesarios
2 Administrar oportunamente todos los cambios en los derechos de acceso (creación, modificación y eliminación), basándose únicamente en transacciones aprobadas y documentadas que hayan sido autorizadas por personas designadas por la dirección.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de administrar cambios de acceso recae sobre la gerencia de tecnología de la información.
3 Segregar, reducir al mínimo necesario y gestionar activamente cuentas de usuario privilegiadas. Asegurar la supervisión de todas las actividades en estas cuentas.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de gestionar cuentas de usuario recae sobre la gerencia de tecnología de la información.
4 Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información. Coordinarse con las unidades de negocio para asegurarse de que todos los roles están definidos de manera consistente, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de procesos del negocio.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de controlar los roles recae sobre la gerencia de tecnología de la información.
5 Autenticar todo el acceso a activos de información de acuerdo con el rol del individuo o a las reglas del negocio. Coordinarse con las unidades de negocio que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos de negocio, con el fin de asegurar que los controles de autenticación hayan sido administrados adecuadamente.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de autenticar todo acceso recae sobre la gerencia de tecnología de la información.
6 Garantizar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación de negocio, infraestructura de TI, operaciones, desarrollo y mantenimiento de sistemas) se puedan identificar de manera unívoca.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de garantizar la identificación de usuarios recae sobre la gerencia de tecnología de la información.
7 Mantener un registro de auditoría del acceso a la información dependiendo de su sensibilidad y de los requisitos regulatorios.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de mantener un registro recae sobre la gerencia de tecnología de la información.
8 Llevar a cabo revisiones gerenciales periódicas de todas las cuentas y privilegios relacionados.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de realizar revisiones recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 05 - Gestionar el acceso físico a los activos de I&T.
Indicadores Asociados: a. Calificación promedio de las evaluaciones de seguridad física

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de registrar y monitorizar recae sobre la gerencia de tecnología de la información.
2 Asegurar que todo el personal muestra una identificación debidamente autorizada en todo momento	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de asegurar la identificacion recae sobre la gerencia administrativa.
3 Requerir a los visitantes que estén acompañados en todo momento durante su estancia en las instalaciones.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura,	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de asegurar la identificacion recae sobre la gerencia administrativa.
4 Restringir y monitorizar el acceso a instalaciones sensibles de TI, mediante el establecimiento de restricciones al perímetro, como vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de asegurar la identificacion recae sobre la gerencia de seguridad.
5 Gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de gestionar permisos de acceso recae sobre la gerencia de tecnología de la información.
6 Garantizar que los perfiles de acceso permanezcan actualizados. Basar el acceso a las instalaciones de TI (sala de servidores, edificios, áreas o zonas) en el cargo y las responsabilidades.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de permisos de acceso actualizados recae sobre la gerencia de tecnología de la información.
7 Realizar formación sobre concienciación de la seguridad de la información física de forma regular.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos tres veces al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de formar recae sobre el funcionario asignado al puesto de gerencia de tecnología de la información, con matriz de cursos gratuitos brindados en la propuesta como referencia.

Práctica de Gobierno (gestión): 06 -Gestionar documentos sensibles y dispositivos de salida.
Indicadores Asociados: a. Número de dispositivos de salida robados.

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Establecer procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura,	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se desarrollan 20 controles de seguridad, los 20 controles mas necesarios
2 Asegurar que se han establecido controles criptográficos para proteger información sensible almacenada electrónicamente.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de controles criptográficos recae sobre la gerencia de tecnología de la información.
3 Asignar privilegios de acceso a documentos sensibles y dispositivos de salida con base en el principio de menor privilegio, manteniendo un equilibrio entre el riesgo y los requisitos del negocio.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de permisos de acceso recae sobre la gerencia de tecnología de la información.
4 Establecer un inventario de documentos sensibles y dispositivos de salida y realizar reconciliaciones periódicas.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de inventario recae sobre la gerencia de tecnología de la información.
5 Establecer salvaguardas físicas adecuadas para documentos sensibles.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de salvaguardar recae sobre la gerencia de seguridad.

Práctica de Gobierno (gestión): 07 - Gestionar las vulnerabilidades y monitorizar la infraestructura
Indicadores Asociados: a. Número de pruebas de vulnerabilidad llevadas a cabo en dispositivos perimetrales

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Usar de forma continua un portafolio de tecnologías, servicios y activos soportados (p. ej., escáneres de vulnerabilidad, fuzzers y sniffers, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se debe contar con el apoyo de gerencia general y gerencia de tecnologia de la informacion
2 . Definir y comunicar escenarios de riesgo para que se puedan reconocer con facilidad y se pueda entender su probabilidad e impacto.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de definir y comunicar recae sobre la gerencia de tecnología de la información.
3 Revisar regularmente los logs de eventos para detectar posibles incidentes.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de revisar logs recae sobre la gerencia de tecnología de la información.
4 Garantizar que se creen tickets relativos a incidentes de seguridad de forma oportuna cuando la monitorización identifique posibles incidentes.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de revisar los tickets recae sobre la gerencia de tecnología de la información.
5 Registrar eventos relacionados con la seguridad y conservar los registros durante el periodo de tiempo apropiado.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de registrar eventos recae sobre la gerencia de tecnología de la información.

- DSS06: Gestión delos controles de procesos de negocio

Se utilizará en el objetivo DSS06 las políticas y buenas prácticas de COBIT2019 para la implementación de un sistema de gestión de seguridad de información (SGSI), donde se aplicarán los siguientes controles:

1. Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.
2. Controlar el procesamiento de información.
3. Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.
4. Gestionar errores y excepciones.
5. Asegurar la trazabilidad y la rendición de cuentas de los eventos de información.
6. Asegurar los activos de información.

Tabla 10 - Matriz DSS06 Sitec Seguridad

Regresar a Inicio

Matriz Guía para la Implementación de Buenas prácticas Basadas en Cobit 2019
Ficha Implementación de Objetivo de Gobierno/Gestión

Sitec Sistemas Integrados de Seguridad S.A.

Dominio: Entregar, dar servicio y soporte

Objetivo de Gestión: DSS06 -Gestionar los controles de procesos de negocio

Proceso relacionado del Marco Normativo: Gobernanza de TI

Riesgos Asociados:

Práctica de Gobierno (gestión): 01 - Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.

Indicadores Asociados:
a. Porcentaje de inventario de procesos críticos y controles clave completado
b. Porcentaje de controles de procesamiento alineados con las necesidades empresariales

Prioridad de Implementación: Etapa 1

Implementable	Porcentaje Avance	Fecha Conclusión Implementación
		3/5/2027

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Identificar y documentar las actividades de control necesarias para procesos clave del negocio para satisfacer los requisitos de control para los objetivos estratégicos, operativos, de reporte y de cumplimiento.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de identificar y documentar recae sobre la gerencia de tecnología de la información.
2 Priorizar las actividades de control de acuerdo al riesgo inherente al negocio. Identificar controles clave.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se debe contar con el apoyo de gerencia general y gerencia de tecnologia de la informacion
3 Garantizar la propiedad de las actividades de control clave.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de garantizar la propiedad recae sobre la gerencia de tecnología de la información.
4 Implementar controles automáticos.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de implementar controles recae sobre la gerencia de tecnología de la información.
5 Monitorizar continuamente las actividades de control de principio a fin para identificar oportunidades de mejora.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.
6 Mejorar de forma continua el diseño y operación de los controles de proceso del negocio.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se debe contar con el apoyo de gerencia general y gerencia de tecnologia de la informacion

Práctica de Gobierno (gestión): 02 -Controlar el procesamiento de información.
Indicadores Asociados: a. Número de incidentes y hallazgos de auditoría que indican un fallo de los controles clave

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Autenticar al originador de las transacciones y comprobar que el individuo tiene la autoridad para originar la transacción	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.
2 Garantizar una adecuada segregación de tareas con relación al origen y aprobación de las transacciones.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.
3 Comprobar que las transacciones son precisas, completas y válidas. Los controles podrían incluir secuencia, límite, rango, validez, razonabilidad, comprobación de tablas, existencia, verificación de clave, dígito de verificación, completitud, comprobaciones de duplicados y relaciones lógicas y ediciones temporales. Los criterios y parámetros de validación deberían estar sujetos a revisiones y confirmaciones periódicas. Validar los datos de entrada y editarlos o, cuando sea aplicable, devolverlos para su corrección lo más cerca posible del punto de origen.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.
4 Sin comprometer los niveles de autorización de la transacción original, corregir y reenviar los datos que se introdujeron de forma errónea. Cuando sea adecuado para la reconstrucción, conservar documentos fuente originales durante el periodo de tiempo adecuado.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.
5 Mantener la integridad y la validez de los datos durante el ciclo de procesamiento. Asegurar que la detección de transacciones erróneas no interrumpe el procesamiento de transacciones válidas.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.
6 Manipular el resultado de forma autorizada, entregarlo al destinatario adecuado y proteger la información durante la transmisión. Verificar la exactitud e integridad del resultado.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.
7 Mantener la integridad de los datos durante interrupciones inesperadas en el procesamiento del negocio. Confirmar la integridad de los datos después de fallos en el procesamiento.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.
8 Antes de pasar datos de transacciones entre aplicaciones internas y funciones operativas/de negocio (dentro o fuera de la empresa), comprobar el trato adecuado, la autenticidad del origen y la integridad del contenido. Mantener la autenticidad y la integridad durante la transmisión o el transporte.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de monitorear recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 03 -Gestionar roles, responsabilidades, privilegios de acceso y
Indicadores Asociados: a. Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funciones

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Asignar roles y responsabilidades conforme a las descripciones del cargo y las actividades aprobadas del proceso de negocio.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de asignar roles recae sobre la gerencia de tecnología de la información.
2 Asignar niveles de autoridad para la aprobación de transacciones, límites de transacción y cualquier otra decisión relacionada con el proceso de negocio, conforme a roles de trabajo aprobados.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de definir niveles de autoridad recae sobre la gerencia de tecnología de la información.
3 Asignar roles para actividades sensibles para que haya una clara segregación de funciones.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de asignar roles recae sobre la gerencia de tecnología de la información.
4 Asignar derechos de acceso y privilegios basado en lo mínimo requerido para realizar las actividades laborales, conforme a roles de trabajo predefinidos. Eliminar o revisar derechos de acceso de forma inmediata si el rol de trabajo cambia o si un miembro del personal deja el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso sea adecuado para las amenazas, riesgo, tecnología y necesidades empresariales actuales.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de asignar derechos de acceso recae sobre la gerencia de tecnología de la información.
5 Concienciar y formar regularmente sobre los roles y responsabilidades, para que todos entiendan sus responsabilidades; la importancia de los controles; y la seguridad, integridad, confidencialidad y privacidad de la información de la compañía en todas sus formas	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se recomienda dentro del proyecto dar capacitaciones almenos con frecuencia de cutrimestral o semestral
6 Garantizar que los privilegios administrativos están asegurados, rastreados y controlados de forma suficiente y eficaz para prevenir el mal uso.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de garantizar privilegios recae sobre la gerencia de tecnología de la información.
7 Revisar periódicamente las definiciones de control de acceso, los logs y los informes de excepción. Asegurar que todos los privilegios de acceso son válidos y están alineados con los miembros actuales del personal y sus roles asignados.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de revisar periodicamente recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 04 -Gestionar errores y excepciones.
Indicadores Asociados: a. Frecuencia de las ineficiencias de procesamiento debido a entradas de datos incompletas

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Revisar errores, excepciones y desviaciones.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de revisar recae sobre la gerencia de tecnología de la información.
2 Hacer un seguimiento, corregir, aprobar y reenviar los documentos fuente y las transacciones.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de seguimiento y otros recae sobre la gerencia de tecnología de la información.
3 Mantener evidencia de acciones correctivas.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de mantener evidencia recae sobre la gerencia de tecnología de la información.
4 Definir y mantener procedimientos para asignar la propiedad de errores y excepciones, corregir errores, anular errores y manejar condiciones fuera del balance.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de definir y mantener recae sobre la gerencia de tecnología de la información.
5 Informar de manera oportuna sobre errores relevantes de procesamiento de la información del negocio para realizar un análisis de causa raíz y de tendencia	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de informar recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 05 - Asegurar la trazabilidad y la rendición de cuentas de los event
Indicadores Asociados: a. Número de incidentes en los que no se puede recuperar el historial de transacciones

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Obtener la información fuente, evidencias de soporte y el registro de transacciones.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de obtener información recae sobre la gerencia de tecnología de la información.
2 Definir los requisitos de retención de acuerdo a los requisitos del negocio para cumplir con las necesidades operativas, de reportes financieros y de cumplimiento.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de definir requisitos recae sobre la gerencia de tecnología de la información.
3 Disponer de la información fuente, las evidencias de soporte y el registro de las transacciones conforme a la política de retención	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de disponer de información recae sobre la gerencia de tecnología de la información.

Práctica de Gobierno (gestión): 06 -Asegurar los activos de información.
Indicadores Asociados: a. Casos de datos de transacciones sensibles enviados al destinatario erróneo

Actividad	Implementable	Fecha Compromiso Implementación	Estado Implementación	Porcentaje Avance	Funcionarios Responsables	Fecha de Control	Documentación de Referencia	Observaciones
1 Restringir el uso, distribución y el acceso físico a la información de acuerdo con su clasificación.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de restringir recae sobre la gerencia de tecnología de la información.
2 Proporcionar una concienciación y formación adecuada sobre el uso.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	Se recomienda dentro del proyecto dar capacitaciones almenos con frecuencia de cutrimestral o semestral
3 Aplicar las políticas y procedimientos de seguridad para la clasificación y uso aceptable de datos y para proteger los activos de información que están bajo control del negocio.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de aplicar politicas recae sobre la gerencia de tecnología de la información.
4 Identificar e implantar procesos, herramientas y técnicas para verificar el cumplimiento de forma razonable.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de identificar e implantar procesos recae sobre la gerencia de tecnología de la información.
5 Informar al negocio y a otras partes interesadas sobre violaciones y desviaciones.	Sí	5/3/2025	En Proceso		Christian Sancho	Al menos una vez al año, cada vez que se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.	Documentos existentes de la empresa, politicas desarrolladas, COBIT 2019, ISO 27001, ISO 27002	La responsabilidad de informar recae sobre la gerencia de tecnología de la información.

El desarrollo del manual de gestión de seguridad de la información, el cual incluye los 20 controles propuestos por la gerencia de Sitec Seguridad, con el propósito de lograr un cumplimiento inicial de las NORMAS ISO 27001 e ISO 27002, incluidas en el Marco de Referencia COBIT 2019 en sus apartados relacionados con Seguridad y Ciberseguridad, están referenciadas a continuación, con lo que se asegura una gestión adecuada de los riesgos y una protección eficaz de los activos de información de Sitec Seguridad.

Tabla 11 - Controles Sitec Seguridad

Anexo A Tipo de control	Identificador del Anexo A de ISO/IEC 27001:2022	Anexo A Nombre	Nombre Control
Controles organizacionales	Anexo A 5.1	Políticas de Seguridad de la Información	A5.1.01.2025
Controles organizacionales	Anexo A 5.12	Clasificación de la información	A5.12.01.2025
Controles organizacionales	Anexo A 5.17	Información de autenticación	A5.17.01.2025
Controles organizacionales	Anexo A 5.18	Derechos de acceso	A5.18.01.2025
Controles organizacionales	Anexo A 5.9	Inventario de Información y Otros Activos Asociados	A5.9.01.2025
Controles de personas	Anexo A 6.3	Concientización, educación y capacitación sobre seguridad de la información	A6.3.01.2025
Controles de personas	Anexo A 6.6	Acuerdos de confidencialidad o no divulgación	A6.6.01.2025
Controles físicos	Anexo A 7.10	Medios de almacenamiento	A7.10.01.2025
Controles físicos	Anexo A 7.14	Eliminación segura o reutilización del equipo	A7.14.01.2025
Controles físicos	Anexo A 7.2	Entrada Física	A7.2.01.2025
Controles físicos	Anexo A 7.3	Seguridad de oficinas, habitaciones e instalaciones	A7.3.01.2025
Controles físicos	Anexo A 7.9	Seguridad de los activos fuera de las instalaciones	A7.9.01.2025
Controles Tecnológicos	Anexo A 8.1	Dispositivos terminales de usuario	A8.1.01.2025

Controles Tecnológicos	Anexo A 8.13	Copia de seguridad de la información	A8.13.01.2025
Controles Tecnológicos	Anexo A 8.15	Inicio de sesión	A8.15.01.2025
Controles Tecnológicos	Anexo A 8.2	Derechos de acceso privilegiados	A8.2.01.2025
Controles Tecnológicos	Anexo A 8.20	Seguridad de Redes	A8.20.01.2025
Controles Tecnológicos	Anexo A 8.3	Restricción de acceso a la información	A8.3.01.2025
Controles Tecnológicos	Anexo A 8.5	Autenticación Segura	A8.5.01.2025
Controles Tecnológicos	Anexo A 8.7	Protección contra malware	A8.7.01.2025

Fuente: Propuesta Sitec Seguridad

Manual de procedimientos para el departamento de tecnología de la información

	SITEC SISTEMAS INTEGRADOS DE SEGURIDAD S.A		**Código: A5.1.01.2025**
	MANUAL GENERAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		**Versión: 1**
			Página 1/
Solicitud de cambio N°: 0	**Elaborado por: Roberto Valverde Quesada**	**Aprobado por: En espera…**	**Rige a partir de: Ver página**

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Ilustración 47 - Política de seguridad de la información

(Capitalis, 2019)

INTRODUCCIÓN:

La política de seguridad de la información es fundamental en la seguridad informática, está diseñada para dar protección, confidencialidad, integridad y disponibilidad a la información de la empresa Sitec Seguridad contra robos y accesos no autorizados.

Se considera esta política como establecimiento de directrices y principios para la protección de activos, es responsabilidad de todos los colaboradores de la empresa Sitec

Seguridad, tomar las precauciones necesarias, las mejores prácticas y cumplir la misma de manera más adecuada, así como la revisión periódica de la misma si se producen cambios en el entorno de seguridad de la información.

PROPÓSITO:

El propósito de esta política es proporcionar a los colaboradores, la gerencia de la empresa Sitec Seguridad y partes externas (por ejemplo, clientes y proveedores) un marco para administrar, proteger los activos, la información electrónica, redes informáticas, así como los procedimientos que deben seguirse para realizar cambios periódicos.

Todo esto tiene como principal objetivo fomentar una cultura de seguridad, reducir el riesgo de pérdida de datos debido a las amenazas internas y externas de la empresa Sitec Seguridad, a través de la sensibilización y el rol de cada persona en la protección de la información con lo que se refuerza la seguridad global de la empresa frente a cualquier intento de accesos no autorizado.

ALCANCE:

La presente política establece que su cumplimiento es obligatorio para todos los colaboradores internos y externos (clientes y proveedores) de Sitec Seguridad, así como para aquellos que gestionen, accedan, obtengan, utilicen, protejan o procesen información confidencial, la misma se extiende a contratistas, consultores, socios comerciales y cualquier tercero que acceda a los sistemas en sus instalaciones, utilice la red de la compañía o almacene información no pública.

La política se aplica a todos los procesos y sistemas de información que se maneja dentro de la empresa, incluyendo colaboradores, proveedores, contratistas, infraestructura, documentos físicos, electrónicos, bases de datos, redes, cualquier otro medio que acceda, procese, almacene o gestione activos de información, lo que asegura el cumplimiento de las normativas y la protección de la información sensible.

DOCUMENTOS APLICABLES:

- Anexo A 5.1 ISO/IEC 27001:2022
- ISO/IEC 27001:2022 – Sistemas de gestión de la seguridad de la información (SGSI)
- ISO/IEC 27002:2022 – Código de buenas prácticas para la gestión de la seguridad de la información
- Ley de Protección de la Persona frente al tratamiento de sus datos personales 8968 (art. 5)(Ver anexos).

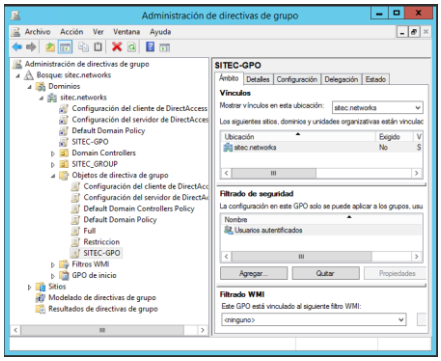
CONTENIDO DE LA POLÍTICA:

Para los propósitos de esta política de la seguridad de la información posee las siguientes directrices:

- La gerencia y/o administración se compromete a aportar los recursos necesarios, para garantizar el cumplimiento de los objetivos de la política de seguridad de la información.
  - Capacitación sobre seguridad de la información y ciberseguridad. (Ver matriz de capacitación en anexos), lo anterior gestionado por el departamento de tecnologías de la información.
  - Desarrollo de protocolos de seguridad para el perfil del usuario a través del controlador de dominio por medio políticas de grupo (GPO); lo anterior gestionado por el departamento de tecnologías de la información.

- Colocación de mensaje de bienvenida al inicio de sesión de los equipos, como recordatorio de la política de privacidad de la información de Sitec Seguridad, lo anterior gestionado por el departamento de tecnologías de la información.

Ilustración 48 - Mensaje de bienvenida



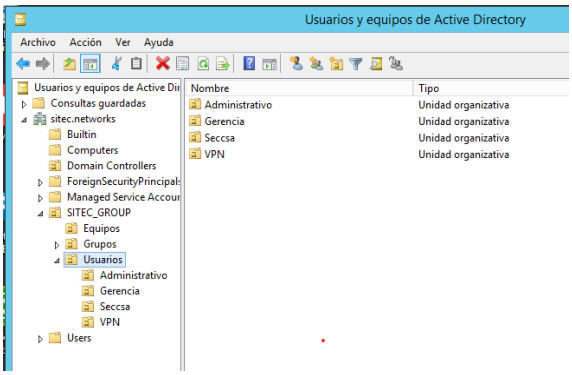
Fuente: Server Sitec Seguridad

- La seguridad de la información es responsabilidad de todos los colaboradores de la empresa Sitec Seguridad los cuales van desde la gerencia hasta los colaboradores operativos.
- Todos los activos de la empresa serán clasificados según el nivel de sensibilidad (confidencial, interno, público, etc.) y deben ser manejados de acuerdo con sus respectivos niveles de protección, lo anterior gestionado por el departamento de tecnologías de la información.
- La empresa llevará a cabo evaluaciones periódicas de riesgos con el fin de identificar, evaluar y mitigar las amenazas que puedan afectar la seguridad de la información.
    - De acuerdo al Marco de Gestión de TI, COBIT 2019 y el ISO/IEC 27001:2022 se recomienda llevar a cabo una evaluación formal **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan**

cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización, lo anterior gestionado por el departamento de tecnologías de la información.

- El acceso a la información de la empresa estará basado en la necesidad de conocimiento, restringido de esta manera a aquellos colaboradores o partes que tengan una razón legítima para acceder a la misma.
- Lo anterior sujeto a los privilegios asignados a su rol (Active Directory), lo anterior gestionado por el departamento de tecnologías de la información.

Ilustración 49 - Active Directory Sitec Seguridad



Fuente: Server Sitec Seguridad

- Los permisos de acceso a la información serán gestionados y revisados periódicamente.
  - Lo anterior sujeto a los privilegios asignados a su rol (Active Directory), lo anterior gestionado por el departamento de tecnologías de la información.

- Se implementarán programas de concientización para todos los colaboradores y partes interesadas sobre la importancia de la seguridad de la información, así como las mejores prácticas para evitar incidentes de seguridad.
    - Flyer ubicados en áreas estratégicas de la empresa (comedor, servicios sanitarios, recepción, entre otros.), lo anterior gestionado por el departamento de talento humano.
    - Por medio de correos electrónicos desarrollados por el departamento de tecnología.
    - Capacitaciones y /o reforzamiento cada 3 a 6 meses o cuando se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización, lo anterior gestionado por el departamento de tecnologías de la información.
- Se realizarán auditorías periódicas de los sistemas de seguridad de la información, con el fin de asegurar que los controles implementados se están siguiendo de manera efectiva y para identificar posibles mejoras en los mismos, lo anterior gestionado por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE INVENTARIO DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

Ilustración 50 - Política de seguridad de inventario de información

(Consulting, 2025)

INTRODUCCIÓN:

Dentro de la gestión de la seguridad de la información, es necesario contar con un inventario completo, preciso de los activos de información y otros activos asociados que Sitec Seguridad posee, gestiona y/o utiliza, la correcta identificación, clasificación y seguimiento de los activos es fundamentales para garantizar su protección y de esa manera reducir riesgos.

Sitec Seguridad reconoce que los activos de información, software, servidores, maquinas, bases de datos, dispositivos de almacenamiento y otros activos asociados, son esenciales para su operación lo que garantiza la continuidad del negocio.

PROPÓSITO:

El propósito de esta política es proporcionar a los colaboradores, la gerencia de la empresa Sitec Seguridad los lineamientos para la identificación, clasificación, gestión, protección de todos los activos de información, así como cualquier otro activo asociados dentro de Sitec Seguridad, con el único fin de garantizar que los mismos se gestionen adecuadamente a lo largo de todo su ciclo de vida, reduciendo de esta manera los riesgos asociados, reforzando la seguridad global de la empresa.

ALCANCE:

Esta política aplica a todos los activos de información, dispositivos, recursos asociados a Sitec Seguridad como lo son:

- Bases de datos (información alojada de los clientes de Sitec Seguridad).
- Documentos (administrativos y clientes).
- Registros electrónicos (facturación a clientes).
- Aplicaciones (MSO365)
- Dispositivos informáticos (laptops y pc).
- Servidores (Active Directory, facturación, bases de datos).
- Equipos de red (L2 y L3).
- Equipos de almacenamiento de datos (sistema de almacenamiento externo).
- Dispositivos móviles (Smartphone y Tablets).
- Personal que gestiona y/o tiene acceso a los activos de información.

La política es aplicable y establece que su cumplimiento es obligatorio para todos los colaboradores, colaboradores internos y externos (clientes y proveedores) de Sitec Seguridad y cualquier otra persona que interactúe con los activos de la empresa

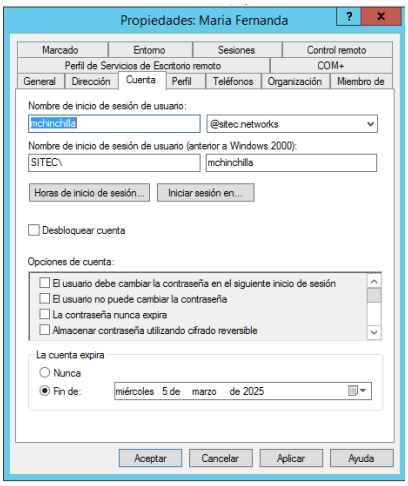
DOCUMENTOS APLICABLES:

- ISO/IEC 27001:2022: Requisitos para un sistema de gestión de seguridad de la información.
- ISO/IEC 27002:2022: Código de buenas prácticas para la gestión de la seguridad de la información.
- Anexo A.5.9 de la ISO 27001:2022: Inventario de información y otros activos asociados.
- Política de Seguridad de la Información de la Organización. Código: A5.1.01.2025

CONTENIDO DE LA POLÍTICA:

- Todos los activos de información de Sitec Seguridad deben ser identificados y catalogados de manera detallada, describiéndolos junto con su ubicación, el propietario, el acceso autorizado al mismo y el uso que se les da, lo anterior gestionado por el departamento de tecnologías de la información.

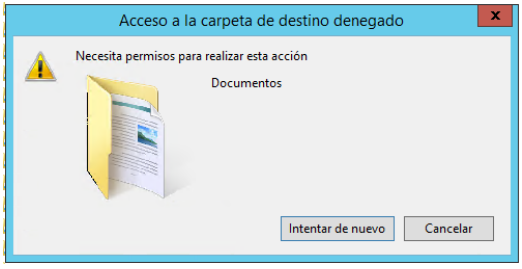
Ilustración 51 - Propiedades Acceso



Fuente: Server Sitec Seguridad

- Los activos de información deben ser clasificados según su importancia para Sitec Seguridad, con su sensibilidad y nivel de protección que requieren (por ejemplo, información confidencial, restringida, pública), lo anterior gestionado por el departamento de tecnologías de la información.

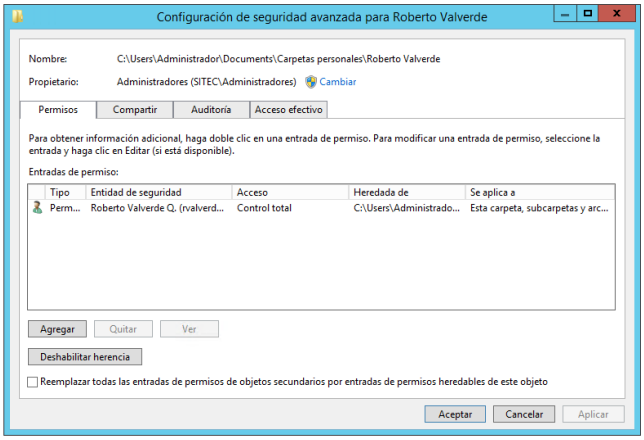
Ilustración 52 - Acceso denegado



Fuente: Server Sitec Seguridad

- Cada activo de información debe tener un propietario definido, este es el responsable de su gestión y de la protección del mismo, lo anterior gestionado por el departamento de tecnologías de la información.

Ilustración 53 - Propietario definido



Fuente: Server Sitec Seguridad

- El propietario del activo deberá garantizar que sea adecuadamente protegido y gestionado conforme a las políticas y procedimientos internos de Sitec Seguridad.
- Los activos de información serán gestionados a lo largo de su ciclo de vida útil, incluyendo desde la adquisición hasta la disposición final, lo anterior gestionado por el departamento de tecnologías de la información.
- Cuando los activos de información dejen de ser necesarios, serán eliminados de manera segura con el único fin de evitar la exposición de información confidencial y/o sensible

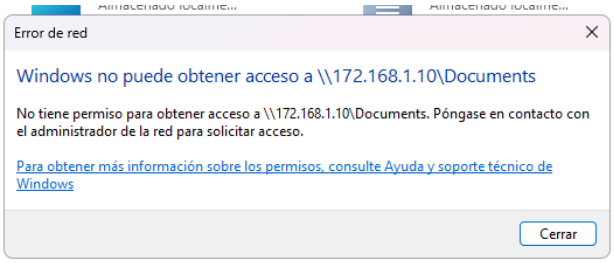
de Sitec Seguridad (incluye la destrucción física y el borrado seguro de datos), lo anterior gestionado por el departamento de tecnologías de la información.

  - Métodos: trituración, incineración o desmagnetización (degaussing) certificada.
  - En el caso de discos duros HD, se deben desmontar y destruir los platos y otros componentes críticos.
  - Dispositivos de estado sólido (SSD), destrucción física mencionada anteriormente para asegurar la eliminación total de los datos.
  - Certificación: Es recomendable que la destrucción se realice a través de proveedores especializados que puedan emitir un certificado de destrucción, garantizando que el dispositivo ha sido procesado conforme a las mejores prácticas y normativas vigentes. Ejemplo: Empresa Valu Shred ubicados en Zona Franca Zeta, Montecillos de Alajuela.

- Se realizarán evaluaciones de riesgos periódicas para identificar los posibles riesgos asociados a la pérdida, daño o acceso no autorizado a los activos de información, lo anterior gestionado por el departamento de tecnologías de la información.
  - De acuerdo al Marco de Gestión de TI, COBIT 2019 y el ISO/IEC 27001:2022 se recomienda llevar a cabo una evaluación formal **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.
- El acceso a los activos de información está restringido únicamente a personal autorizado y claramente definido con controles dentro de las políticas de acceso basadas en el

principio de mínimo privilegio, lo anterior gestionado por el departamento de tecnologías de la información.

Ilustración 54 - Restricción de acceso



Fuente: Server Sitec Seguridad

- Todos los accesos a estos activos deben ser monitoreados y auditados regularmente para detectar actividades no autorizadas a los mismos, lo anterior gestionado por el departamento de tecnologías de la información.
- El inventario de activos debe mantenerse actualizado en todo momento.
    - Tanto por el departamento contable como por el departamento de gestión de tecnologías, de tal manera que se conozca que equipos siguen activos en la empresa.
- Los cambios en los activos, como la compra, traslado, remplazo o eliminación, deben registrarse de inmediato en el inventario.
    - Será responsabilidad del departamento de gestión tecnologías registrar las nuevas compras, traslados, remplazo o eliminación de activos, manteniendo el inventario actualizado en todo momento.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE CLASIFICACION DE LA INFORMACION

Ilustración 55 - Política de clasificación de la información

(Excelencia, 2019)

INTRODUCCIÓN:

Dentro de clasificación de la información es un componente crítico para garantizar la confidencialidad, integridad y disponibilidad de los activos informáticos de Sitec Seguridad, a través de un proceso clave que permite proteger los datos, gestionarlos de manera adecuada y cumplir con los requisitos legales y regulatorios, la política establece los requisitos mínimos para la clasificación de la información según su nivel de sensibilidad y el impacto que tendría su divulgación no autorizada de la misma.

PROPÓSITO:

El propósito de clasificación de la información es establecer directrices claras para clasificar, agrupar y manejar los activos de la información dentro de Sitec Seguridad, de acuerdo con la sensibilidad, requisitos legales, valor, criticidad y el riesgo asociado a la divulgación o modificación no autorizada, la clasificación permitirá darles una adecuada protección a los activos informáticos y asegurará la implementación de controles apropiados en función de la

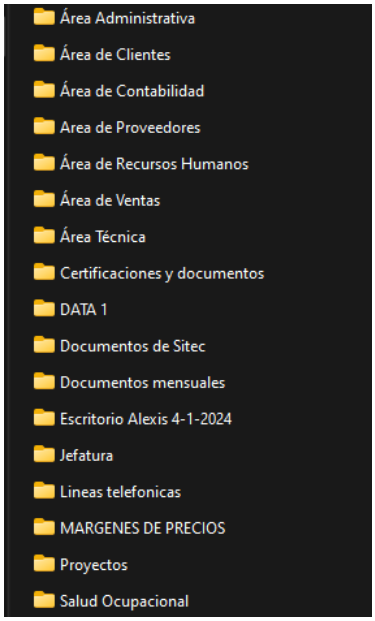
naturaleza de la información, reduciendo de esta manera los riesgos asociados, reforzando la seguridad global de la empresa.

ALCANCE:

Esta política aplica a todos colaboradores, contratistas, proveedores y cualquier otra parte interesada que tenga acceso a la información de Sitec Seguridad, sea esta física o digital y cubre todos los tipos de información generada y administrada por la empresa, como lo son:

- Datos confidenciales
- Registros financieros
- Propiedad intelectual
- Registros de proveedores
- Clientes
- Información de colaboradores
- Otros.

Ilustración 56 - catalogo de información



Fuente: Server Sitec Seguridad

DOCUMENTOS APLICABLES:

- ISO/IEC 27001:2022, Anexo A – Control A.5.12: Clasificación de la Información.
- Acuerdo de confidencialidad para colaboradores de Sitec Seguridad.
- Política de ciberseguridad de Sitec Seguridad.
- Política de Seguridad de la Información de la Organización. Código: A5.1.01.2025

CONTENIDO DE LA POLÍTICA:

La información será clasificada en diferentes categorías según su nivel de sensibilidad:

- Confidencial es aquella información que, si es revelada, podría causar daño significativo a Sitec Seguridad o sus partes interesadas, lo anterior gestionado por el departamento administrativo.
- Interna es toda aquella información que es de uso exclusivo e interno a Sitec Seguridad y cuya divulgación podría afectar la eficiencia operativa de la misma, lo anterior gestionado por el departamento administrativo.
- Pública se considera toda la información cuyo acceso y divulgación no representa un riesgo para la Sitec Seguridad, lo anterior gestionado por el departamento de administrativo.

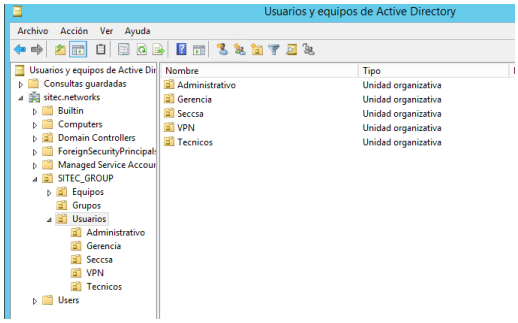
Todos los colaboradores de Sitec Seguridad deben identificar y etiquetar la información asignada según su rol, para darle una clasificación adecuada.

Los colaboradores deben tener acceso a la información solo dentro de los límites de su responsabilidad, de acuerdo a su rol y según la necesidad de conocimiento de la misma.

- Lo anterior sujeto a los privilegios asignados a su rol (Active Directory), lo anterior gestionado por el departamento de tecnologías de la información.

El acceso de información considerada como clasificada, será restringida a únicamente personas autorizadas, y estos permisos deben ser revisados periódicamente, lo anterior gestionado por el departamento de tecnologías de la información.

Ilustración 57 - Segmentación de usurios

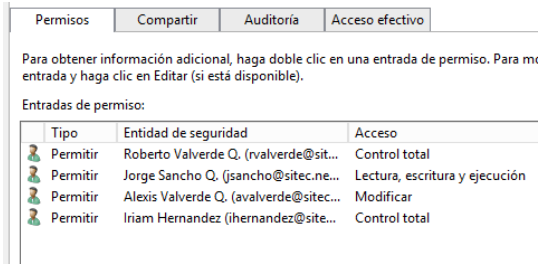


Fuente: Server Sitec Seguridad

Los sistemas de control de acceso a la información deberán ser configurados para permitir y garantizar solo el acceso autorizado a la información clasificada según los niveles de seguridad definidos por roles.

- Lo anterior sujeto a los privilegios asignados a su rol (Active Directory), lo anterior gestionado por el departamento de tecnologías de la información.

Ilustración 58 - Permisos de usuario



Fuente: Server Sitec Seguridad

La información ya clasificada debe ser almacenada de forma segura, tanto en medios electrónicos como físicos de Sitec Seguridad. lo anterior gestionado por cada usuario según su rol.

Todos aquellos medios que contengan información confidencial deben ser destruidos de manera segura al final de su ciclo de vida, lo anterior gestionado por el departamento de tecnologías de la información.

- Métodos: trituración, incineración o desmagnetización (degaussing) certificada.
- En el caso de discos duros HD, se deben desmontar y destruir los platos y otros componentes críticos.
- Dispositivos de estado sólido (SSD), destrucción física mencionada anteriormente para asegurar la eliminación total de los datos.
- Certificación: Es recomendable que la destrucción se realice a través de proveedores especializados que puedan emitir un certificado de destrucción, garantizando que el dispositivo ha sido procesado conforme a las mejores prácticas y normativas vigentes. Ejemplo: Empresa Valu Shred ubicados en Zona Franca Zeta, Montecillos de Alajuela.

Los cambios en información, creación, modificación o eliminación, deben registrarse y darles el tratamiento de clasificación adecuado, lo anterior gestionado por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE INFORMACIÓN DE AUTENTICACIÓN

Ilustración 59 - Política de información de autenticación

(Jessyca, 2021)

INTRODUCCIÓN:

Las contraseñas desempeñan un rol fundamental en la seguridad informática, estás constituyen la primera capa de protección para todas las cuentas de usuario, si las contraseñas no son seguras y adecuadas, ponen en peligro toda la infraestructura de red de la empresa, lo que tiene efectos graves para la seguridad y operación de Sitec Seguridad.

Se considera responsabilidad de todos los colaboradores de la empresa Sitec Seguridad, tomar las precauciones necesarias para seleccionar y almacenar sus contraseñas de manera más adecuada.

PROPÓSITO:

El propósito de esta política es establecer un conjunto de directrices para la creación de contraseñas seguras, de tal manera que las contraseñas sean lo suficientemente fuertes y eficaces para contrarrestar posibles amenazas internas y/o externas, se detallan medidas necesarias para

proteger adecuadamente estas contraseñas, así como los procedimientos que deben seguirse para realizar cambios periódicos.

Todo esto tiene como principal objetivo reducir el riesgo de que un atacante interno y/o externo que haya obtenido una contraseña antigua, pueda acceder a los sistemas y datos sensibles de la empresa Sitec Seguridad, con lo que se refuerza la seguridad global de la empresa frente a cualquier intento de accesos no autorizado.

ALCANCE:

La presente política establece que su cumplimiento es obligatorio para todos los colaboradores de Sitec Seguridad, así como para aquellos que gestionen, accedan, obtengan, utilicen, protejan o procesen información confidencial, la misma se extiende a contratistas, consultores, socios comerciales y cualquier tercero que tenga un dispositivo móvil proporcionado por la empresa, acceda a los sistemas en sus instalaciones, utilice la red de la compañía o almacene información no pública.

La información que se maneja dentro de la empresa está sujeta a las leyes y regulaciones de protección de datos del estado costarricense, así como a los acuerdos internacionales vigentes en esta materia, lo que asegura el cumplimiento de las normativas y la protección de la información sensible.

DOCUMENTOS APLICABLES:

- Ley 8454, Ley de Certificados, Firmas Digitales y documentos electrónicos (artículo 6°, ver anexos)
- Ley 9048 Ref. 9135, Ley de Delitos Informáticos y Conexos (artículo 229 bis, ver anexos)

- Política de seguridad de la información Código A.5.1.01.2025.
- Procedimiento de Autenticación Multifactor (MFA).

CONTENIDO DE LA POLÍTICA:

Directrices:

Para los propósitos de esta política, las contraseñas tienen varios propósitos, siendo algunos de los usos más comunes y frecuentes: cuentas de usuario para acceder Windows, cuentas de acceso en línea, cuentas de correo electrónico, protección del protector de pantalla, contraseñas de teléfonos y accesos a sistemas de información internos.

Los principios, directrices y políticas de la empresa son aplicables tanto a las actividades en línea como a otras áreas del entorno laboral.

A. **Las contraseñas débiles tienen las siguientes características:**
   - La contraseña se compone de menos de ocho caracteres.
   - La contraseña es encontrable en un diccionario.
   - La contraseña es una palabra de uso común como: nombre de un familiar, mascota, amigos, compañeros, etc.
   - Contraseñas usadas en términos informáticos, comandos, sitios, empresas, hardware, software.
   - Palabras como “Trabajo”, “Casa”, “hola” o derivaciones.
   - Cumpleaños u otra información personal como teléfonos o direcciones.
   - Palabras y/o números en patrones como abc123, qwerty, 123321, etc.

B. **Las contraseñas seguras tienen las siguientes características:**

- Se combinan caracteres en mayúsculas y minúscula, por ejemplo, a-z, A-Z
- Tienen dígitos y caracteres de puntuación, así como símbolos, ejemplo 0-9, @#$%&*_-+[]{}^'¿?!¡\ < > /, ; . :
- Mínimo poseen ocho caracteres alfanuméricos y se recomienda 10 caracteres como mínimo
- No son una palabra escrita en cualquier idioma, dialecto, jerga, etc.
- No se basan en información personal como nombres de familia, amigos, etc.
- Las contraseñas seguras nunca deben ser escritas o almacenadas en línea.

Trate de crear contraseñas que se puedan recordar fácilmente, una forma de hacer esto es crear una contraseña basada en un título, afirmación o frase, por ejemplo, "Contraseña" la misma podría ser "C0ntr4s3n4" o "C0ntr4s3n4.#" o alguna variación.

NOTA: No utilice cualquier de los ejemplos dados como contraseña propia.

C. **Normas de protección con contraseña:**

- No usar la misma contraseña para cuentas empresariales y personales.
- No utilice la misma contraseña para diferentes necesidades de acceso en el lugar donde labora.
- Selecciones una contraseña independiente para su cuenta de Windows y otra para su cuenta de correo electrónico.
- No comparta las contraseñas de trabajo o personales a nadie, incluyendo amigos, compañeros o jefes.
- Todas las contraseñas deben ser tratadas confidencialmente ya que son información sensible.

Aquí esta una lista de “lo que **no** debe hacer”:

- No revelar la contraseña por teléfono a nadie que solicite la misma.
- No revelar la contraseña en un mensaje de texto y/o correo electrónico.
- No revelar la contraseña al compañero de trabajo y/o jefe.
- No conversar de su contraseña enfrente de los demás.
- No insinuar o dar indicios del formato de una contraseña.
- No revelar una contraseña en cuestionarios y/o formularios de seguridad.
- No compartir la contraseña empresarial con miembros de la familia.
- No revelar contraseñas a compañeros y/o jefes mientras este de vacaciones.

Si alguien solicita su contraseña debe de remitirlo a este documento y comunicarse con personal del departamento de tecnologías de la información, para el seguimiento respectivo.

- No utilice la función “recordar contraseña” en ninguna aplicación, navegador o sistema de mensajería que utilice.
- Nuevamente recuerde nunca escribir la contraseña en papel y/o almacenarla en un lugar de la oficina.
- No guarde las contraseñas intente memorizarlas.
- Cambie las contraseñas al menos una vez cada 90 días, a excepción de contraseñas de nivel de sistema que deben ser cada 60 días.
- Si sospecha que su cuenta o cualquier contraseña ha sido comprometida se debe de reportar el incidente al departamento de TI y cambiar todas las contraseñas.
- Lo anterior gestionado por cada usuario al recibir su equipo y revisado el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE DERECHO DE ACCESO

Ilustración 60 - Política de derecho de acceso

(STUDIO, s.f.)

INTRODUCCIÓN:

La gestión adecuada de los derechos de acceso es un aspecto fundamental para garantizar la seguridad de la información dentro de Sitec Seguridad, un acceso no autorizado a sistemas, aplicaciones o datos sensibles puede poner en riesgo la confidencialidad, integridad, disponibilidad de la información de la empresa, el objetivo es establecer principios y directrices para la gestión y control de los derechos de acceso, asegurando que solo las personas autorizadas puedan acceder a los recursos adecuados de acuerdo con su rol y responsabilidades, se basa en el control A.8.18 de la norma ISO/IEC 27001:2022, que establece las directrices para los derechos de acceso dentro la organización.

PROPÓSITO:

El propósito de esta política es definir el enfoque de Sitec Seguridad para gestionar los derechos de acceso de los usuarios a los sistemas de información, datos, recursos, su implementación garantizará que se cumplan los principios de seguridad de "mínimos privilegios"

y "necesidad de saber", permitiendo solo el acceso necesario para el desempeño de las funciones laborales y protegiendo la información de accesos indebidos o malintencionados.

La gestión adecuada de los derechos de acceso es fundamental para proteger los activos de información de la empresa, así como garantizar que los recursos se utilicen de manera segura y eficiente, a través de la implementación de esta política Sitec Seguridad asegura que los accesos sean apropiados, controlados, auditados, minimizando los riesgos de accesos no autorizados y contribuyendo a la protección integral de la información.

ALCANCE:

Esta política es aplicable a todos los usuarios de los sistemas informáticos, redes de la empresa, incluidos empleados, contratistas, consultores y otros terceros que requieran acceso a los recursos de información, cubre el acceso a todos los sistemas de información, aplicaciones, bases de datos, redes y dispositivos de la organización, tanto en entornos de trabajo como remotos, los derechos de acceso deberán ser gestionados de acuerdo con las directrices de esta política y de acuerdo con el rol funcional de cada usuario.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Sistema de gestión de seguridad de la información (SGSI), Anexo A.5.18 - Derechos de acceso.
- Política de seguridad de la información Código A.5.1.01.2025.

- Política general de información de autenticación Código A5.17.01.2025.
- Política de Derechos de acceso privilegiados Código: A8.2.01.2025.

CONTENIDO DE LA POLÍTICA:

Gestión de la Asignación de Derechos de Acceso

Los derechos de acceso deben asignarse basándose en el principio de "necesidad de saber", es decir, solo se otorgará acceso a los recursos que sean esenciales para el desempeño de las funciones del usuario.

- Lo anterior sujeto a los privilegios asignados a su rol (Active Directory), lo anterior gestionado por el departamento de tecnologías de la información.

Los derechos de acceso deben ser evaluados y aprobados por los responsables del área o sistema pertinente antes de ser otorgados.

Los usuarios deben ser categorizados según su rol dentro de la empresa, el acceso a la información debe ser restringido según la clasificación de los recursos y la sensibilidad de los datos, lo anterior gestionado por el departamento administrativo.

- Confidencial es aquella información que, si es revelada, podría causar daño significativo a Sitec Seguridad o sus partes interesadas.
- Interna es toda aquella información que es de uso exclusivo e interno a Sitec Seguridad y cuya divulgación podría afectar la eficiencia operativa de la misma.
- Pública se considera toda la información cuyo acceso y divulgación no representa un riesgo para la Sitec Seguridad.

- Lo anterior sujeto a los privilegios asignados a su rol (Active Directory), lo anterior gestionado por el departamento de tecnologías de la información.

Proceso de Revisión y Modificación de Derechos de Acceso

Los derechos de acceso deben ser revisados periódicamente para asegurarse de que los usuarios mantienen acceso solo a los recursos necesarios para sus funciones, la revisión debe llevarse a cabo al menos una vez al año o cuando se produzcan cambios significativos en las funciones o responsabilidades de los usuarios.

Cualquier modificación en el rol de un usuario, como ascensos, traslados o finalización de contrato, debe implicar una actualización de los derechos de acceso correspondientes.

La revocación de derechos de acceso debe ser inmediata en el caso de que un usuario abandone la empresa o cambie de rol, para evitar accesos no autorizados.

Lo anterior es gestionado por el departamento de tecnologías de la información.

Control de Acceso Físico y Lógico

El acceso físico a áreas sensibles debe estar restringido mediante el uso de tarjetas de acceso, biometría o cualquier otro mecanismo de control físico.

- Puertas con restricción de acceso y controladas con sistemas físicos o electrónicos.

El acceso lógico debe ser protegido mediante el uso de contraseñas robustas, autenticación multifactor (MFA) y otras medidas de seguridad apropiadas.

- También la utilización de sistemas de seguridad como alarmas y cctv.

El acceso a sistemas críticos debe ser limitado a personal con permisos especiales y debe ser registrado en los registros de auditoría para su posterior revisión.

Lo anterior es gestionado por el departamento de tecnologías de la información.

Implementación del Principio de Mínimos Privilegios

Cada usuario debe recibir el menor nivel de acceso posible para realizar su trabajo de manera eficaz.

Los derechos de acceso para los administradores de sistemas deben estar restringidos y gestionados bajo estrictas políticas de control.

Lo anterior es gestionado por el departamento de tecnologías de la información.

Autenticación y Control de Contraseñas

Se debe implementar un sistema de autenticación robusto, que incluya políticas de contraseñas seguras y mecanismos de autenticación multifactor cuando sea posible, lo anterior gestionado por el departamento de tecnologías de la información.

- Política general de información de autenticación A5.17.01.2015

Las contraseñas deben ser cambiadas regularmente y deben cumplir con los requisitos mínimos de longitud y complejidad.

En el caso de acceso remoto, se deben implementar medidas adicionales de control de acceso y cifrado para proteger los datos transmitidos, lo anterior gestionado por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

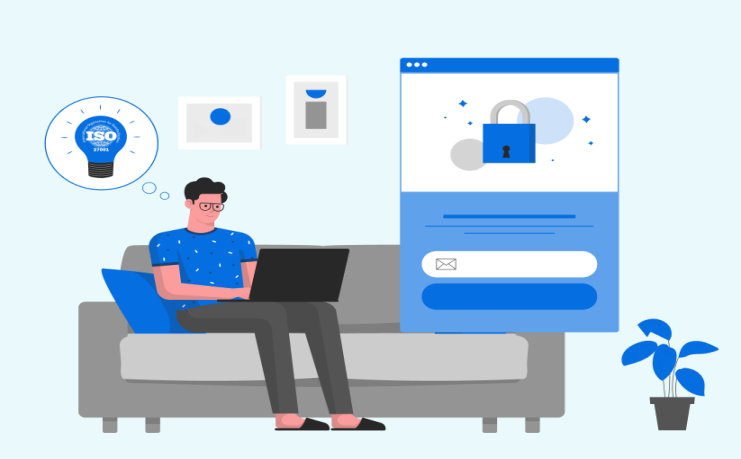
ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE CONCIENTIZACIÓN, EDUCACIÓN Y CAPACITACIÓN SOBRE SEGURIDAD DE LA INFORMACIÓN

Ilustración 61 - Política de concientización y capacitación



(Araujo, s.f.)

INTRODUCCIÓN:

La concientización, educación y capacitación sobre la seguridad de la información es un componente esencial para la protección de los activos de información dentro de Sitec Seguridad, lo que implica informar a los colaboradores la importancia y dada la naturaleza los riesgos asociados con el acceso no autorizado, el uso indebido, la divulgación de la información, de ahí la importancia, ya que es fundamental que todos los colaboradores y partes interesadas comprendan su responsabilidad en la protección de la información, así como de los peligros cibernéticos que existen.

PROPÓSITO:

El propósito de esta política es proporcionar a los colaboradores, gerencia y partes externas (por ejemplo, clientes y proveedores) información y concientización de los riesgos asociados con el acceso no autorizado, el uso indebido, la divulgación de la información y la responsabilidad en la protección de la información, a través de:

- Fomentar una cultura empresarial orientada a la seguridad de la información.
- Asegurar que todos los colaboradores de Sitec Seguridad, desde el personal ejecutivo hasta los colaboradores operativos, comprendan la importancia de proteger la información y la infraestructura tecnológica de la empresa.
- Garantizar que los colaboradores reciban formación continua y actualizada para identificar, prevenir y reaccionar ante incidentes de seguridad.
- Reducir los riesgos asociados, reforzando la seguridad global de la empresa.

ALCANCE:

Esta política aplica a todos los colaboradores, contratistas, proveedores y cualquier otra parte interesada de la empresa, sin importar su nivel jerárquico o función.

Todos aquellos contratistas o proveedores que tengan acceso a los activos de información de Sitec Seguridad e interactúen de alguna manera con los mismos.

Cualquier otra parte interesada con acceso o interacción con los sistemas físicos, digitales y la infraestructura de información de la empresa.

Está política abarca cualquier actividad relacionada con la seguridad de la información, incluye la protección de datos, el acceso a los sistemas, la gestión de incidentes y la seguridad en las comunicaciones de Sitec Seguridad.

DOCUMENTOS APLICABLES:

- Anexo A6.3 de ISO/IEC 27001:2022 – Concientización, educación y capacitación sobre seguridad de la información.
- Política de Seguridad de la Información de la Organización. Código: A5.1.01.2025.

CONTENIDO DE LA POLÍTICA:

La política busca desarrollar conciencia en los colaboradores de la importancia de la seguridad de la información de la siguiente manera:

- Realización de campañas periódicas de sensibilización, lo anterior gestionado por el departamento de tecnologías de la información cada 3 meses.
- Comunicaciones constantes de las amenazas emergentes, lo anterior gestionado por el departamento de tecnologías de la información cada vez que sea necesario.
    - Por medio de correos electrónicos desarrollados por el departamento de tecnología.
- Recordatorios, posters, avisos de seguridad en áreas comunes, lo anterior gestionado por el departamento de talento humano.
- Entrenamientos cortos de refrescamiento (por ejemplo, videos, charlas, flyers, entre otros) sobre temas claves, emergentes o actualizaciones, lo anterior gestionado por el departamento de tecnologías de la información y coordinado con talento humano, cada vez que sea necesario.
    - Flyer ubicados en áreas estratégicas de la empresa (comedor, servicios sanitarios, recepción, entre otros.).

- Capacitaciones y /o reforzamiento cada 3 a 6 meses o cuando se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización

- Proporcionando conocimientos sobre las políticas, los procedimientos y las mejores prácticas en seguridad, desarrollados por el departamento de tecnologías de la información.
- Impartiendo cursos para la protección de datos, ciberseguridad y gestión de accesos en general desarrollados por el departamento de tecnología de la información u otras compañías.
    - Capacitación sobre seguridad de la información y ciberseguridad. (Ver matriz de capacitación en anexos).
- Realizando simulaciones de ciberataques o ejercicios de phishing a los colaboradores, desarrollados por el departamento de tecnología de la información.
- Recibiendo formación especializada para áreas clave como lo son: departamento de tecnologías de la información. y administrativa, (Ver matriz de capacitación en anexos).
- Capacitando al personal en la manera correcta de aplicar los controles de seguridad en el desarrollo de sus tareas diarias por el departamento de tecnología de la información.
- Se implementarán evaluaciones periódicas en la empresa que permitan medir la efectividad de las actividades de concientización y capacitación, (Ver matriz de capacitación en anexos).

- Realización de encuestas de retroalimentación, exámenes o pruebas sobre los contenidos formativos, desarrollados por el departamento de tecnologías de la información cada 3 meses.
- Se incorporarán nuevas herramientas y métodos de formación, como plataformas de Viva Learning, para facilitar el acceso a la capacitación, desarrollados por el departamento administrativo.

Ilustración 62 - Viva learning Sitec Seguridad

Fuente: Office 365 Seguridad

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización. Debido a la importancia de proteger los activos y la información sensible,

cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente. La evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN

Ilustración 63 - Política de confidencialidad o no divulgación

(WebMaster, 2023)

INTRODUCCIÓN:

La confidencialidad de cualquier información es fundamental en la gestión de la seguridad de la información de Sitec Seguridad, proteger la información sensible, evitar su divulgación no autorizada, es esencial que todos los colaboradores, contratistas y terceros que tengan acceso a información confidencial de Sitec Seguridad, deban firmar acuerdos de confidencialidad o no divulgación, en los cuales se establecen las obligaciones de las partes involucradas para garantizar la protección de los datos y la información en todo momento, ya sea durante así como después de la relación laboral o contractual.

PROPÓSITO:

El propósito de esta política es establecer directrices para la creación, gestión, cumplimiento de los acuerdos de confidencialidad y la no divulgación dentro y fuera de Sitec Seguridad, asegurando que todos los colaboradores, contratistas, proveedores y terceros comprendan sus obligaciones legales y contractuales en relación con la protección de la información confidencial de la empresa.

La política garantiza una correcta implementación de controles necesarios para prevenir la divulgación no autorizada de información sensible, así como establecer un marco formal y legal para la protección de la información por partes externas como proveedores y socios comerciales de Sitec Seguridad.

ALCANCE:

Todos los colaboradores de la organización, independientemente de su nivel jerárquico o área funcional, contratistas, consultores y proveedores todos los que tengan acceso a información confidencial o que estén involucrados en la gestión de datos sensibles de Sitec Seguridad son alcanzados por esta política, así como:

- Todos aquellos terceros que mantengan de una u otra manera relaciones contractuales con la organización y a su vez tengan acceso o manipulen información confidencial de Sitec Seguridad.
- La política abarca la firma, revisión y ejecución de acuerdos de confidencialidad de Sitec Seguridad, así como todas las obligaciones derivadas de los mismos.

DOCUMENTOS APLICABLES:

- Anexo A6.6 de ISO/IEC 27001:2022 – Acuerdos de confidencialidad o no divulgación.
- Política de Seguridad de la Información de la Organización. Código: A5.1.01.2025.
- Acuerdo de confidencialidad para manejo de la información Sitec Seguridad.

CONTENIDO DE LA POLÍTICA:

La política busca establecer un marco claro y legalmente vinculante que respalde la confidencialidad de la información, garantizando que los colaboradores, contratistas y terceros entiendan sus responsabilidades de la siguiente manera:

- Se entiende como compromiso de no divulgar, comentar, compartir o permitir el acceso a información clasificada como confidencial a ninguna persona no autorizadas o

relacionada con la misma, de acuerdo con las políticas y normativas internas de Sitec Seguridad, gestionado por el departamento administrativo.

- La no divulgación de la información incluye el compromiso de no hacer pública por ningún medio, así como el no compartir información sensible con terceros sin el consentimiento explícito de la parte interesada y autorizado por escrito por parte de Sitec Seguridad.
- Los colaboradores, contratistas, proveedores y terceros deben firmar un acuerdo de confidencialidad antes de tener acceso a información sensible, lo que incluye el acceso a datos personales, estados financieros, propiedad intelectual, estrategias de desarrollo, estrategias comerciales, y cualquier otro tipo de información clasificada como confidencial, gestionado por el departamento administrativo.
- La duración de la obligación de confidencialidad es de 2 años y debe mantenerse incluso después de que termine la relación laboral o contractual con Sitec Seguridad, gestionado por el departamento administrativo.
- Ningún colaborador o tercero podrá acceder a información confidencial sin haber firmado previamente el acuerdo de confidencialidad correspondiente.
    - El acuerdo será verificado por el departamento administrativo ante una solicitud previa, gestionado por el departamento administrativo.
- Sitec Seguridad llevará un registro adecuado de todos los acuerdos de confidencialidad firmados, asegurando que puedan ser consultados y verificados en cualquier momento, gestionado por el departamento administrativo.

- Los acuerdos serán resguardados según la política seguridad de oficinas, habitaciones o instalaciones.

- Se implementarán medidas para garantizar el cumplimiento de los acuerdos, como lo son auditorías periódicas o los controles de acceso a la información confidencial, gestionado por el departamento administrativo.
- Al concluir la relación laboral o contractual, el colaborador o tercero deberá devolver o destruir la información confidencial que posea o tenga acceso dentro de los términos acordados en el contrato, gestionado por el departamento de tecnologías de la información.
    - Aplicando la política de eliminación segura o reutilización de equipos.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE ENTRADA FISICA

Ilustración 64 - Política de entrada física

(SitecSeguridad, 2010)

INTRODUCCIÓN:

La seguridad física es un componente clave de la protección de los activos de información de Sitec Seguridad, todo acceso físico no controlado a las instalaciones compromete

la seguridad de la infraestructura tecnológica, los datos sensibles y todos aquellos recursos considerados valiosos, es necesario establecer controles sobre el acceso físico a las instalaciones como lo son puertas, portones, lectores de acceso, escáneres biométricos, llaveros y especialmente en áreas sensibles, con el propósito de prevenir accesos no autorizados, sabotajes, robos o alteraciones a la infraestructura o datos.

PROPÓSITO:

La política de entrada física tiene como objetivo regular, así como controlar el acceso físico a las instalaciones y áreas críticas de Sitec Seguridad, garantizando que solo el personal autorizado pueda ingresar a áreas consideradas como restringidas.

Esta establece controles claros para el control del acceso físico a las instalaciones de la organización, logrando minimizar los riesgos asociados con el acceso no autorizado a las áreas sensibles y así protegiendo los activos de información mediante controles que eviten comprometer la infraestructura física o los datos.

Se debe implementar el uso de cerraduras manuales o electrónicas, sistemas de seguridad que permitan restringir, controlar, registrar todo ingreso o intento de ingreso autorizado o no autorizado en las áreas sensibles de la empresa.

ALCANCE:

Todos los colaboradores de Sitec Seguridad, independientemente de su nivel jerárquico o área funcional que necesiten acceso físico a las instalaciones están considerados como lo son:

- Contratistas, proveedores y visitantes que puedan tener acceso a las instalaciones o requieran acceso a las áreas sensibles.
- Otras partes interesadas que requiera acceso físico para la realización de actividades relacionadas con la operación de la empresa, por ejemplo, proveedor de servicios de internet y/o telefonía.
- El alcance cubre todas las instalaciones físicas de Sitec Seguridad, incluidos los edificios, salas de servidores, centros de datos, áreas de almacenamiento de información confidencial (física o digital) y otros espacios considerados críticos.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- Anexo A7.2 de ISO/IEC 27001:2022 – Control de acceso físico a las instalaciones.
- Política de Seguridad de la Información de la Organización. Código: A5.1.01.2025.

CONTENIDO DE LA POLÍTICA:

La política busca establecer un marco claro que garantice el acceso autorizado a las áreas por parte de los colaboradores, contratistas y terceros.

Áreas Sensibles:

Estás se identificarán y clasificarán como: centros de datos, oficinas de alta dirección, laboratorios de desarrollo de software, bodegas de equipos y otros lugares donde se almacenen o procesen datos críticos de Sitec Seguridad.

El acceso a áreas sensibles solo estará permitido a aquel personal autorizado con la formación adecuada y previamente registrado en los sistemas de control de acceso correspondientes al área (físicos o electrónicos).

El acceso a las instalaciones se controlará mediante tecnologías adecuadas, como lectores biométricos y/o contraseña, gestionado por el departamento de tecnologías de la información.

Los visitantes no serán registrados en ningún sistema de control de acceso.

Los visitantes serán acompañados por un empleado autorizado y tendrán acceso restringido a áreas específicas, a su vez deben registrarse en la entrada, proporcionar identificación válida (al día) y firmar un acuerdo de confidencialidad, en caso de ser necesario, controlado por el departamento administrativo.

Los colaboradores tendrán acceso asignado a las instalaciones de acuerdo con su rol y responsabilidades, gestionado por el departamento administrativo.

Los accesos de colaboradores deben ser revocados inmediatamente cuando el colaborador cambie de puesto o termine su relación laboral, gestionado por el departamento administrativo.

Los contratistas y proveedores tendrán acceso físico a las instalaciones de acuerdo con los términos establecidos por los cuales fueron contratados, gestionado por el departamento administrativo.

El acceso de contratistas y proveedores será supervisado y limitado a las áreas necesarias para la realización de su trabajo, bajo supervisión un responsable con acceso al área, gestionado por el departamento administrativo.

Todos los accesos a las instalaciones o áreas sensibles serán registrados, manualmente o a través de sistemas automatizados.

Los registros deben incluir nombre, identificación del empleado, contratista o visitante, así como la hora de entrada y salida, y el propósito de visita.

Se establecerán sistemas de monitoreo físico, como cámaras de seguridad (existentes), para supervisar el acceso a las instalaciones y áreas sensibles, gestionado por el departamento de tecnologías de la información.

Los sistemas de video vigilancia estarán configurados para alertar a los responsables de seguridad en caso de incidentes inusuales en dichas áreas, gestionado por el departamento de seguridad.

Todo el material, equipo, dato sensible o confidencial que se extraiga de Sitec Seguridad será verificado y registrado, de acuerdo con los procedimientos de seguridad establecidos en las políticas A5.9.24.01.2025 y A5.12.24.01.2025, gestionado por el departamento administrativo. Y revisado por el departamento de tecnologías de la información.

Se llevarán a cabo auditorías periódicas para evaluar la efectividad de los controles de acceso físico, incluye los registros de acceso y la verificación de cumplimiento de los controles establecidos, gestionado por el departamento de seguridad.

Los sistemas de control de accesos físicos serán revisados periódicamente, especialmente cuando cambien las funciones o rol de los colaboradores, contratos con proveedores y/o contratistas, gestionado por el departamento de seguridad.

Cualquier intento de acceso no autorizado a un área sensible será considerado un incidente de seguridad y será tratado según el procedimiento de respuesta a incidentes, se debe notificar inmediatamente a los responsables y, si es necesario, hasta la intervención de autoridades competentes.

En situaciones de emergencia, como temblores, incendios o evacuaciones, se garantizará que los controles de acceso físico se adapten para permitir una evacuación rápida y segura de los colaboradores, a la vez que se mantienen los controles necesarios para evitar accesos no deseados a las áreas sensibles.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del

departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

	SITEC SISTEMAS INTEGRADOS DE SEGURIDAD S.A		**Código: A7.3.01.2025**
	MANUAL GENERAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		**Versión: 1**
			Página 1/
Solicitud de cambio N°: 0	**Elaborado por: Roberto Valverde Quesada**	**Aprobado por: En espera…**	**Rige a partir de: Ver página**

POLÍTICA GENERAL DE SEGURIDAD DE OFICINAS, HABITACIONES E INSTALACIONES

Ilustración 65 - Política de seguridad de oficinas e instalaciones

(CEC, 2020)

INTRODUCCIÓN:

La seguridad física y ambiental de las oficinas, habitaciones e instalaciones es fundamental para proteger los activos de la organización, garantizar la confidencialidad, integridad y disponibilidad de la información, así como asegurar el bienestar de nuestros colaboradores. La implementación de medidas de seguridad es un componente esencial para

cumplir con los requisitos de la norma ISO/IEC 27001:2022, en particular el control A.7.3, que establece directrices para la protección física de las instalaciones y la gestión de riesgos asociados a la seguridad del entorno laboral.

PROPÓSITO:

El propósito de esta política es definir las medidas y controles necesarios para garantizar la seguridad física de las instalaciones y oficinas de la empresa Sitec Seguridad. Se busca proteger la infraestructura, los recursos de información y el personal frente a accesos no autorizados, daños, amenazas externas e incidentes relacionados con la seguridad física, además, establece los lineamientos necesarios para asegurar la continuidad de las operaciones, minimizando riesgos y daños potenciales.

La seguridad física de las instalaciones y oficinas de la empresa Sitec Seguridad es un componente crucial dentro de la gestión de la seguridad de la información, esta política establece las directrices necesarias para proteger los recursos, garantizar la continuidad del negocio, donde todos los colaboradores y partes interesadas deben adherirse a estas medidas para asegurar la protección de la empresa contra amenazas externas e internas, promoviendo un entorno seguro y controlado.

ALCANCE:

Esta política aplica a todas las instalaciones y oficinas que forman parte de la empresa, incluyendo áreas de acceso restringido y sensibles, lo anterior incluye, pero no se limita a:

- Oficinas principales.

- Centros de datos.
- Almacenes de equipos y recursos.
- Zonas de almacenamiento de información confidencial.
- Áreas administrativas y de talento humanos.

Asimismo, esta política es aplicable a todo el personal, contratistas y visitantes que ingresen a las instalaciones, tiene vigencia en todas las áreas de la empresa donde se maneje información sensible o se realicen actividades críticas.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar e aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Control A.7.3 (Seguridad física y del entorno)
- Política de seguridad de la información Código A.5.1.24.01.2025
- Política de entrada física A7.2.01.2025.

CONTENIDO DE LA POLÍTICA:

Control de acceso físico:

- Se implementarán sistemas de control de acceso y/o cctv en todas las instalaciones críticas, como oficinas, salas de servidores y almacenes de datos, gestionado por el departamento de seguridad.

- Sólo se permitirá el acceso a personas autorizadas mediante el uso de tarjetas de identificación, sistemas biométricos u otros mecanismos de autenticación adecuados, gestionado por el departamento de seguridad.
- Se llevará un registro detallado de todas las entradas y salidas de personas a las instalaciones para auditoría y control.

Zonas restringidas o áreas de alto riesgo:

- Las áreas de alto riesgo, como las salas de servidores, deberán contar con acceso restringido y contar con un sistema de monitoreo continuo.
- Las zonas que almacenen información confidencial o equipos sensibles estarán protegidas por cerraduras y sistemas de alarmas, gestionado por el departamento de seguridad.

Seguridad de los edificios:

- Los edificios deben ser diseñados y mantenidos para prevenir accesos no autorizados.
- Las entradas principales y secundarias estarán equipadas con sistemas de seguridad como cámaras de vigilancia y alarmas, gestionado por el departamento de seguridad.
- Las puertas de acceso a áreas restringidas deben estar siempre cerradas y sólo podrán abrirse con autorización expresa, gestionado por el departamento administrativo.

Protección contra desastres y contingencias:

- Las instalaciones deben contar con sistemas de protección contra incendios, inundaciones, terremotos u otros desastres naturales que puedan afectar la integridad de los activos y la seguridad física.

- Se establecerán controles claros para la evacuación del personal en caso de emergencia, gestionado por el departamento administrativo.

Control de visitantes:

- Todos los visitantes deberán registrarse en la entrada de las instalaciones y ser acompañados por personal autorizado en todo momento durante su estancia.
- No se permitirá el acceso de personas a áreas sensibles sin la supervisión adecuada.

Seguridad en el perímetro:

- El perímetro de las instalaciones debe ser vigilado continuamente mediante la utilización de cámaras de seguridad, cercas perimetrales y otros mecanismos disuasorios contra intrusiones, gestionado por el departamento de seguridad.

Mantenimiento de las instalaciones:

- Las instalaciones deben ser mantenidas en óptimas condiciones para garantizar la seguridad del entorno físico, evitando daños estructurales o cualquier otra condición que pueda comprometer la seguridad, gestionado por el departamento administrativo.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la empresa. Debido a la importancia de proteger los activos y la información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente. La evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES

Ilustración 66 - Política de seguridad de los activos fuera de las instalaciones

(SEAM, 2023)

INTRODUCCIÓN:

La gestión de activos fuera de las instalaciones es un aspecto clave dentro de la estrategia de seguridad de la información, el manejo de activos con acceso a la información como: dispositivos electrónicos, documentos sensibles y otros recursos críticos, que se encuentran fuera de las instalaciones deben ser protegidos adecuadamente para minimizar el riesgo de acceso no autorizado, pérdida o daño, la política se basa en el control A.7.9 de la norma ISO/IEC 27001:2022, que establece las directrices necesarias para asegurar la protección de los activos fuera de las instalaciones físicas de la empresa, particularmente cuando estos se encuentran bajo la custodia de colaboradores o contratistas.

PROPÓSITO:

El propósito de esta política es definir las medidas y controles necesarios para garantizar la seguridad de los activos que se encuentran fuera de las instalaciones de la empresa Sitec Seguridad, con el objetivo de proteger la información confidencial, evitar el acceso no autorizado, prevenir pérdidas, daños y garantizar la integridad de los activos mientras estén fuera del entorno controlado de la empresa.

La seguridad de los activos fuera de las instalaciones es un componente esencial de la estrategia global de gestión de la seguridad de la información, por lo cual la política establece las directrices necesarias para proteger los activos de la empresa, garantizando su integridad, confidencialidad y disponibilidad, incluso cuando se encuentren fuera del entorno seguro de las instalaciones.

El cumplimiento de estas directrices es esencial para minimizar los riesgos asociados a la pérdida o robo de información y proteger la empresa frente a amenazas externas.

ALCANCE:

Esta política aplica a todos los activos de la empresa que puedan estar fuera de las instalaciones físicas, incluyendo, pero no limitándose a:

- Equipos portátiles (laptops, Smartphone, tablets).
- Dispositivos de almacenamiento extraíbles (USB, discos duros portátiles).
- Documentos físicos o archivos confidenciales que se manejen fuera de las instalaciones.
- Equipos y documentos transportados por colaboradores o contratistas a su lugar de trabajo o fuera de Sitec Seguridad.

Adicionalmente la política aplica a todo el personal, contratistas y cualquier tercero que tenga acceso o sea responsable de estos activos fuera de las instalaciones de la empresa.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Control A.7.9 (Seguridad de los activos fuera de las instalaciones)
- Política de seguridad de la información Código A.5.1.01.2025.
- Política de inventario de información y otros activos asociados A5.9.01.2025.
- Política de derechos de acceso A5.18.01.2025.
- Política acuerdos de confidencialidad o no divulgación A6.6.01.2025.

- Política de autenticación segura A8.5.01.2025.
- Política de inicio de sesión A8.15.01.2025.
- Procedimiento de Protección de Información Confidencial.

CONTENIDO DE LA POLÍTICA:

Protección de Activos Portátiles:

- Todos los dispositivos electrónicos, como laptops, teléfonos móviles y tablets, que contengan información sensible, deben ser protegidos mediante contraseñas fuertes, autenticación multifactor (MFA) y encriptación de los datos almacenados, lo anterior será revisado por el departamento de tecnologías de la información.
- El uso de dispositivos portátiles para almacenar información sensible está restringido, y se debe seguir un procedimiento específico de seguridad para el acceso y uso de los mismos fuera de las instalaciones, lo anterior será revisado por el departamento de tecnologías de la información.

Encriptación de Información Sensible:

- Toda la información que se transporte fuera de las instalaciones (en dispositivos portátiles o medios físicos) debe ser encriptada para prevenir el acceso no autorizado en caso de pérdida o robo de los dispositivos, lo anterior será revisado por el departamento de tecnologías de la información.
    - La encriptación debe cumplir con los estándares de la empresa y las mejores prácticas de la industria para garantizar un nivel adecuado de protección.

Control de Transporte y Almacenamiento de Activos Fuera de las Instalaciones:

- Los documentos físicos que contengan información confidencial o sensible deben ser transportados en condiciones que aseguren su protección, como el uso de maletines cerrados y seguros, o a través de empresas de mensajería que cuenten con mecanismos de seguridad adecuados, lo anterior es gestionado por el departamento administrativo.
- Los documentos no deben ser dejados en lugares públicos o en áreas no aseguradas durante el transporte o almacenamiento temporal fuera de las instalaciones, lo anterior es responsabilidad de cada usuario.

Uso de Medios de Almacenamiento Externo:

- Los medios de almacenamiento extraíbles (USB, discos duros portátiles) solo deben usarse para transportar datos esenciales y deben ser protegidos por contraseña y encriptación, lo anterior es revisado por el departamento de tecnologías de la información.
- El uso de servicios de almacenamiento en la nube está sujeto a la aprobación de la empresa, y se debe verificar que dichos servicios cumplan con los requisitos de seguridad de la información, lo anterior es revisado por el departamento de tecnologías de la información.

Acceso y Gestión de Dispositivos:

- Solo se permitirá el acceso a dispositivos portátiles a aquellas personas que estén autorizadas, y dichos dispositivos deberán ser configurados de manera que solo se

pueda acceder a la información con las credenciales apropiadas, lo anterior es revisado por el departamento de tecnologías de la información.

- Se debe implementar una política de bloqueo remoto y borrado de datos en caso de pérdida o robo de dispositivos portátiles, de forma que se pueda garantizar la destrucción de la información sensible, lo anterior es revisado por el departamento de tecnologías de la información.

La empresa llevará a cabo auditorías periódicas para verificar que los activos fuera de las instalaciones se gestionen de acuerdo con esta política y las mejores prácticas de seguridad, gestionado por el departamento de tecnologías de la información cada 3 meses.

Los registros de transporte y acceso a los activos fuera de las instalaciones serán monitoreados para garantizar el cumplimiento de los controles establecidos, revisados por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la empresa, debido a la importancia de proteger los activos y la información sensible,

cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente. La evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE MEDIOS DE ALMACENAMIENTO

Ilustración 67 - Política de medios de almacenamiento

(pxhere, s.f.)

INTRODUCCIÓN:

Los dispositivos portátiles deben garantizar la protección de la información que contienen almacenada y se procesan en ellos, así como lo indica la norma ISO/IEC27001, aplicando la misma para equipos laptops, unidades usb y teléfonos móviles; convirtiéndose en una de las políticas que reduce riesgos estrictamente relacionados con robo, perdida y/o accesos no autorizados a la información de Sitec Seguridad, la implementación de controles de acceso, cifrado de información y procedimientos seguros para la eliminación de datos.

PROPÓSITO:

El propósito de esta política es establecer un conjunto actividades permitidas o restringidas al utilizar equipos y/o dispositivos de la empresa Sitec Seguridad, controlando los accesos no autorizados, amenazas como malware y divulgación de datos sensibles de la empresa a través de la limitación de uso de estos dispositivos los cuales tienen un fin específico, se define el control de acceso de los dispositivos personales y se solamente se permite a personal autorizado, manteniendo una cultura de seguridad con información de las buenas prácticas y de un uso responsable.

ALCANCE:

La presente política establece que su cumplimiento es obligatorio para todos los colaboradores y colaboradores de Sitec Seguridad, así como para aquellos que gestionen, accedan, obtengan, utilicen, protejan o procesen información confidencial, la misma se extiende a contratistas, consultores, socios comerciales y cualquier tercero que tenga un dispositivo o móvil proporcionado por la empresa, así como todos los que accedan a los sistemas en sus instalaciones, utilice la red de la compañía o almacene información no pública.

La información que se maneja dentro de la empresa está sujeta a las leyes y regulaciones de protección de datos del estado costarricense, así como a los acuerdos internacionales vigentes en esta materia, lo que asegura el cumplimiento de las normativas y la protección de la información sensible.

DOCUMENTOS APLICABLES:

- ISO/IEC 27001:2022: Requisitos para un sistema de gestión de seguridad de la información.
- ISO/IEC 27002:2022: Código de buenas prácticas para la gestión de la seguridad de la información.
- ISO/IEC 27040:2015: Directrices sobre la seguridad de los sistemas de almacenamiento de la información.
- Política de seguridad de la información de Sitec Seguridad Código: A5.1.01.2025
- Política de eliminación segura o reutilización del equipo Código: A7.14.01.2025

CONTENIDO DE LA POLÍTICA:

El personal de la empresa Sitec Seguridad solo puede y debe utilizar medios tipo usb en las computadoras de trabajo, estos medios usb no se pueden ni deben conectar a computadores que no sean de Sitec Seguridad sin el permiso explícito del personal de tecnologías de la información de la empresa, toda información sensible debe ser almacenada en el servidor de datos de la empresa o pc asignada por la misma, y en usb únicamente cuando sea necesario en el desempeño de sus deberes asignados o se deba proporcionar al interesado con las previas

autorizaciones internas de la jefatura de Sitec Seguridad, esta a su vez debe estar cifrada o protegida con una contraseña.

Medios portátiles:

Son aquellos que pueden ser como lo menciona ser trasladados de una computadora a otra sin modificar la misma y en el cual se almacena información, dentro de los medios se encuentran:

- Usb, cámaras, handheld.
- Memoria flash u otro tipo.
- Discos externos mecánicos y/o sólidos.
- Dispositivos ópticos como CD, DVD, Blu-ray

Medios digitales:

Son aquellos que pueden ser como lo menciona ser trasladados de una manera digital en el cual se almacena información, dentro de los medios digitales se encuentran:

- Discos en la nube.
- Servidores de red.
- Bases de datos.

Teléfonos celulares (Smartphone):

La empresa suministra teléfonos celulares (Smartphone) para la recolección de datos y con autorización escrita el uso de dispositivos personales como lo establece la política interna SIT-2024-008 la cual restringe el uso en horario laboral para el personal.

Los medios de almacenamiento serán clasificados según los datos que contienen o van a contener con el fin de aplicar las medidas de seguridad apropiadas de acuerdo a su clasificación.

- El acceso a los medios de almacenamiento está restringido a personal autorizado de acuerdo con los roles y responsabilidades definidos por Sitec Seguridad en su GPO, revisado por el departamento de tecnologías de la información.

Todos los medios de almacenamiento que contengan información sensible o confidencial deben estar cifrados tanto en reposo como en tránsito, revisado por el departamento de tecnologías de la información.

Los datos serán respaldados regularmente a través de medios de almacenamiento seguros.

- Se tratarán de acuerdo a la política de copia de seguridad de la información y revisado por el departamento de tecnologías de la información.

Los respaldos deben custodiarse en ubicaciones separadas y seguras, con el fin de asegurar la disponibilidad de los datos, gestionado por el departamento administrativo.

Los dispositivos de almacenamiento físico deben estar almacenados de manera segura, protegidas contra el acceso no autorizado, el robo y/o el daño físico.

- Se aplicará la política de seguridad de oficinas, habitaciones e instalaciones, gestionado por el departamento de seguridad.

Los dispositivos portátiles (como portátiles, usb, discos duros externos, etc.) deben ser transportados bajo protocolos de seguridad, asegurando su protección contra pérdida o acceso no autorizado de terceros, bajo la responsabilidad del colaborador.

Cuando los medios de almacenamiento ya no sean utilizados o deban ser dados de baja, serán destruidos de tal manera que la información en ellos no pueda ser recuperada, realizado por el departamento de tecnologías de la información.

Se debe incluir procesos de destrucción física y/o eliminación segura de datos en medios de almacenamiento móviles, aplicando tecnologías de borrado seguro que aseguren que los datos no puedan ser recuperados.

- Métodos: trituración, incineración o des magnetización (degaussing) certificada.
- En el caso de discos duros HD, se deben desmontar y destruir los platos y otros componentes críticos.
- Dispositivos de estado sólido (SSD), destrucción física mencionada anteriormente para asegurar la eliminación total de los datos.
- Certificación: Es recomendable que la destrucción se realice a través de proveedores especializados que puedan emitir un certificado de destrucción, garantizando que el dispositivo ha sido procesado conforme a las mejores prácticas y normativas vigentes. Ejemplo: Empresa Valu Shred ubicados en Zona Franca Zeta, Montecillos de Alajuela.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE ELIMINACIÓN SEGURA O REUTILIZACIÓN DEL EQUIPO

Ilustración 68 - Política de eliminación segura

(Group, 2015)

INTRODUCCIÓN:

La gestión adecuada de los equipos y dispositivos al final de su vida útil es esencial para proteger la información sensible y garantizar la seguridad de Sitec Seguridad, por lo que la eliminación segura y/o reutilización de equipos como: ordenadores, discos duros, usb, Smartphone y otros dispositivos, debe llevarse a cabo de manera que se evite la recuperación no autorizada de datos y previniendo incidentes de seguridad o filtraciones de información, la política se basa en el control A.7.14 de la norma ISO/IEC 27001:2022, que establece directrices para la eliminación segura y reutilización de los equipos de forma que se cumplan los requisitos de seguridad de la información.

PROPÓSITO:

La política establece los procedimientos y controles necesarios para la eliminación segura y/o reutilización de los equipos o dispositivos que contengan información sensible, confidencial, asegurando que no sea posible la recuperación no autorizada de datos cuando dichos equipos ya no se necesiten, se vendan, se donen o desechen, el objetivo es minimizar el riesgo de filtraciones de información para proteger la privacidad de los datos gestionados por la empresa.

La eliminación segura y/o reutilización de los equipos es una parte fundamental de la estrategia de seguridad de la información de Sitec Seguridad, siguiendo esta política Sitec Seguridad garantizará que todos los dispositivos y equipos son gestionados de forma adecuada, protegiendo los datos sensibles y evitando filtraciones de información.

ALCANCE:

Esta política aplica a todos los equipos y dispositivos de la empresa que contengan datos sensibles, confidenciales o privados, que deban ser eliminados o reutilizados de forma segura, incluyendo, pero no limitándose a:

- Computadoras de escritorio y portátiles
- Dispositivos móviles (Smartphone, tablets)
- Discos duros, SSDs, y otros dispositivos de almacenamiento
- Equipos de red, servidores y dispositivos periféricos
- Medios extraíbles como CDs, DVDs, USBs, tarjetas de memoria

La política es aplicable a todos los colaboradores, contratistas, proveedores, y cualquier otra persona que tenga acceso a los equipos de la empresa, así como a cualquier equipo que esté siendo gestionado, vendido, donado o desechado.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Control A.7.14 (Eliminación segura o reutilización de equipos)
- Política de seguridad de la información Código A.5.1.24.01.2025
- Política de inventario de información y otros activos asociados Código: A5.9.01.2025
- Acuerdo de confidencialidad para manejo de la información Sitec Seguridad.

CONTENIDO DE LA POLÍTICA:

Los equipos que ya no sean necesarios o que estén fuera de uso deben ser sometidos a un proceso de eliminación de datos que impida su recuperación, incluye la destrucción física o el borrado seguro de los datos, realizado por el departamento de tecnologías de la información.

Los discos duros, SSDs y otros medios de almacenamiento deben ser borrados utilizando herramientas de software especializadas que cumplan con estándares reconocidos (como el estándar DoD 5220.22-M o NIST SP 800-88 (Team, 2024)), realizado por el departamento de tecnologías de la información.

Cuando la eliminación de datos se intente mediante software y no sea viable (por ejemplo, en dispositivos que no se pueden sobrescribir), se deberá proceder con la destrucción física del medio de almacenamiento, como el triturado o el desmagnetizado (destrucción de discos), realizado por el departamento de tecnologías de la información.

- Métodos: trituración, incineración o des magnetización (degaussing) certificada.
- En el caso de discos duros HD, se deben desmontar y destruir los platos y otros componentes críticos.
- Dispositivos de estado sólido (SSD), destrucción física mencionada anteriormente para asegurar la eliminación total de los datos.
- Certificación: Es recomendable que la destrucción se realice a través de proveedores especializados que puedan emitir un certificado de destrucción, garantizando que el dispositivo ha sido procesado conforme a las mejores prácticas y normativas vigentes.

  Ejemplo: Empresa Valu Shred ubicados en Zona Franca Zeta, Montecillos de Alajuela.

Los equipos que se vayan a reutilizar, ya sea dentro de la empresa o fuera de ella (por ejemplo, para donación o venta), deben pasar por un proceso de limpieza exhaustiva que garantice la eliminación de todos los datos sensibles, realizado por el departamento de tecnologías de la información.

- Antes de la reutilización, se debe realizar una evaluación del dispositivo para asegurarse de que los datos no puedan ser recuperados a través de métodos forenses o herramientas especializadas.
- Cualquier dispositivo que vaya a ser reutilizado fuera de la empresa deberá ser limpiado adecuadamente y pasar por un proceso de verificación para garantizar que no contiene información confidencial o sensible.

Para equipos que no puedan ser reutilizados ni revendidos (por ejemplo, equipos obsoletos o dañados), se deberá llevar a cabo una destrucción física completa que impida cualquier intento de recuperación de los datos, realizado por el departamento de tecnologías de la información.

- La destrucción debe ser realizada de acuerdo con los procedimientos específicos establecidos por la empresa, que pueden incluir el triturado de discos duros o el desmantelamiento de otros componentes electrónicos.

Todos los equipos y dispositivos que sean eliminados o reutilizados deben ser registrados en un inventario para asegurar un seguimiento adecuado y la verificación de que los datos se han eliminado de forma segura, realizado por el departamento de tecnologías de la información.

- El registro debe incluir detalles sobre el dispositivo (tipo, modelo, número de serie), el proceso de eliminación o destrucción seguido, y la fecha en que se realizó la acción.

Si se recurre a proveedores externos para la eliminación o destrucción de equipos, estos deben cumplir con los requisitos de seguridad establecidos por la empresa y proporcionar evidencia de que se ha seguido un proceso seguro, solicitado por el departamento de tecnologías de la información.

- Los contratos con proveedores externos deben incluir cláusulas que garanticen la destrucción segura de los datos y la protección de la información durante todo el proceso, verificados con el departamento administrativo.

Los procedimientos para la eliminación segura o reutilización de equipos deben ser revisados periódicamente para asegurarse de que estén actualizados y sigan las mejores prácticas y estándares de la industria, realizado por el departamento de tecnologías de la información.

- Cualquier cambio en la tecnología, legislación o en los requisitos de seguridad de la empresa deberá reflejarse en las actualizaciones de la política y los procedimientos asociados.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

(FANDOM, s.f.)

INTRODUCCIÓN:

La seguridad de los dispositivos terminales de usuario es fundamental para la protección de la información dentro de Sitec Seguridad, los dispositivos terminales, como ordenadores portátiles, estaciones de trabajo, teléfonos móviles, tabletas y otros dispositivos conectados a la red de Sitec Seguridad, son puntos de acceso críticos a los sistemas y datos corporativos, así como la adecuada gestión de estos dispositivos es esencial para mitigar los riesgos de acceso no autorizado, pérdida de datos y ciberamenazas, se basa en el control A.8.1 de la norma ISO/IEC 27001:2022, que establece las directrices para los dispositivos terminales de usuario dentro la organización.

PROPÓSITO:

El propósito de esta política es definir las pautas y controles necesarios para el uso adecuado de los dispositivos terminales de usuario, garantizando la seguridad de la información gestionada y transmitida a través de dichos dispositivos, la política busca:

- Asegurar que todos los dispositivos terminales sean gestionados de forma segura.
- Prevenir el acceso no autorizado a la información y sistemas de la organización.
- Minimizar los riesgos asociados al robo, pérdida o uso indebido de dispositivos terminales.

ALCANCE:

Esta política se aplica a todos los empleados, contratistas y terceros que utilicen dispositivos terminales de usuario en el ámbito de Sitec Seguridad, incluidos, pero no limitando a:

- Computadoras portátiles, de sobremesa y estaciones de trabajo.
- Smartphones y tabletas.
- Cualquier otro dispositivo electrónico que se conecte a los sistemas de información de Sitec Seguridad, como impresoras o dispositivos de almacenamiento extraíbles.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Sistema de Gestión de la Seguridad de la Información (SGSI).
- ISO/IEC 27002:2022 – Código de buenas prácticas para la gestión de la seguridad de la información.

- Política de seguridad de la información Código A.5.1.01.2025.
- Política general de Información de autenticación A5.17.01.2025.
- Política de Concientización, educación y capacitación sobre seguridad de la información A6.3.01.2025.
- Política de seguridad de los activos fuera de las instalaciones A7.9.01.2025.
- Política de protección de malware A8.7.01.25.
- Política de seguridad de redes A8.20.01.2025.

CONTENIDO DE LA POLÍTICA:

Todos los dispositivos terminales de usuario deberán estar registrados ante el departamento de tecnología de la información (TI) y autorizados para su uso en la red corporativa, incluye la revisión periódica de los dispositivos activos y su desconexión en caso de no ser utilizados de manera adecuada, lo anterior y siguiente será verificado por el departamento de tecnología de la información.

- Los dispositivos terminales deben estar protegidos físicamente en todo momento para evitar el acceso no autorizado y en caso de pérdida o robo, el usuario debe notificar inmediatamente al departamento de TI para tomar medidas correctivas.
- Todos los dispositivos terminales deben contar con cifrado de disco completo para proteger la información almacenada en caso de pérdida o robo del dispositivo (incluye laptops, teléfonos móviles y otros dispositivos portátiles).

- Los dispositivos deben contar con medidas de autenticación robustas, como contraseñas, autenticación biométrica o autenticación multifactorial (MFA), para prevenir el acceso no autorizado.
- Las terminales deben mantener actualizados los sistemas operativos y las aplicaciones utilizadas, con la instalación inmediata de actualizaciones de seguridad y parches recomendados por los proveedores de software.
- Los dispositivos deben conectarse solo a redes seguras y controladas por la organización, el uso de redes Wi-Fi públicas o no autorizadas está prohibido para el acceso a los sistemas corporativos.
- Para los dispositivos móviles (smartphones, tabletas), deben implementarse políticas adicionales que incluyan la gestión remota, la protección con contraseñas, y la capacidad de borrar datos de manera remota en caso de pérdida o robo.
- Solo se debe permitir la instalación de software o aplicaciones aprobados por Sitec Seguridad, el uso de software no autorizado está prohibido para minimizar riesgos de seguridad, como malware o vulnerabilidades.
- Los usuarios son responsables de la protección de sus dispositivos terminales, incluida la implementación de medidas de seguridad como contraseñas seguras, bloqueos de pantalla, y la instalación de antivirus si fuera necesario.

Procedimiento en Caso de Incidente

En caso de pérdida, robo o acceso no autorizado a un dispositivo terminal, se debe seguir el procedimiento de respuesta a incidentes de seguridad de la información, que incluye:

- Notificación inmediata al departamento de tecnología de la información y al departamento de seguridad por parte del usuario afectado.
- Desactivación de accesos y redes relacionadas con el dispositivo afectado por parte del departamento de tecnología de la información.
- Investigación para determinar el alcance de la violación de seguridad por parte del departamento de tecnología de la información.
- Recopilación de pruebas y análisis forense, si es necesario por parte del departamento de tecnología de la información y el departamento de seguridad.
- Notificación a las autoridades pertinentes, si corresponde por parte del departamento administrativo.

Sitec Seguridad debe proporcionar formación continua a todos los usuarios sobre la seguridad de los dispositivos terminales, incluyendo buenas prácticas, riesgos asociados y medidas preventivas por parte del departamento de tecnología de la información, además, debe asegurarse de que todos los usuarios comprendan su responsabilidad en el cumplimiento de esta política.

- Se utilizará como guía la política general de concientización, educación y capacitación sobre seguridad de la información Código: A6.3.01.2025

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización. Debido a la importancia de proteger los activos y la información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente. La evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE DERECHOS DE ACCESO PRIVILEGIADOS

Ilustración 70 - Política de derechos de acceso privilegiados

(OCDTECH, s.f.)

INTRODUCCIÓN:

El acceso privilegiado a los sistemas, redes y aplicaciones de la empresa representa un riesgo significativo para la seguridad de la información, dado que permite a los usuarios realizar acciones con permisos elevados, como la administración de sistemas, acceso a información sensible y configuración de dispositivos críticos, la correcta gestión de los derechos de acceso privilegiados es fundamental para minimizar el riesgo de abuso de privilegios, accesos no autorizados, o manipulación maliciosa de datos, la política se basa en el control A.8.2 de la norma ISO/IEC 27001:2022, que establece directrices para la gestión adecuada de los derechos de acceso privilegiados.

PROPÓSITO:

El propósito de esta política es definir los procedimientos y medidas de control necesarias para gestionar, supervisar y proteger los derechos de acceso privilegiados en los sistemas, aplicaciones de la empresa, esto incluye garantizar que solo los usuarios autorizados reciban privilegios elevados y estos se asignen de acuerdo con principios de necesidad, su uso se supervisa de manera continua para prevenir y detectar accesos no autorizados, así como comportamientos inapropiados.

La gestión adecuada de los derechos de acceso privilegiados es fundamental para garantizar la seguridad de los sistemas y la protección de la información sensible dentro de la empresa, la política establece las directrices necesarias para gestionar, controlar, monitorear y auditar los accesos privilegiados, asegurando que solo los usuarios autorizados y en circunstancias adecuadas tengan acceso a los recursos críticos.

ALCANCE:

Esta política aplica a todos los sistemas, aplicaciones y recursos de tecnología de la información de la empresa que cuenten con funciones o permisos privilegiados, tales como:

- Sistemas operativos y plataformas de red.
- Bases de datos (información alojada de los clientes de Sitec Seguridad).
- Equipos de red (L2 y L3).
- Aplicaciones críticas y sistemas de gestión de la información
- Documentos (administrativos y clientes).
- Registros electrónicos (facturación a clientes).
- Aplicaciones (MSO365)
- Dispositivos informáticos (laptops y pc).
- Servidores (Active Directory, facturación, bases de datos).
- Equipos de almacenamiento de datos (sistema de almacenamiento externo).
- Dispositivos móviles (Smartphone y tablets).

La política es aplicable a todos los colaboradores, contratistas y terceros que gestionen o tengan acceso a derechos privilegiados en los sistemas de la empresa, y cubre todos los procesos desde la asignación inicial de privilegios hasta la revocación de los mismos.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Control A.8.2 (Derechos de acceso privilegiados).
- Política de seguridad de la información Código A.5.1.24.01.2025.
- Política de derechos de acceso A5.18.01.2025.

CONTENIDO DE LA POLÍTICA:

Los derechos de acceso privilegiados son asignados exclusivamente a los usuarios que necesiten esos privilegios para el desempeño de sus tareas laborales y de acuerdo con el principio de "mínimos privilegios", es decir, otorgar solo los permisos estrictamente necesarios para realizar las funciones del rol correspondiente.

- La asignación de acceso privilegiado es revisada y aprobada por departamento de tecnología de la información, asegurando que los privilegios sean adecuados y estén bien documentados.

Las cuentas con privilegios elevados, como las de administrador de sistema o súper usuario, son controladas rigurosamente, estas cuentas deben ser identificables y diferenciadas de las cuentas de usuario estándar.

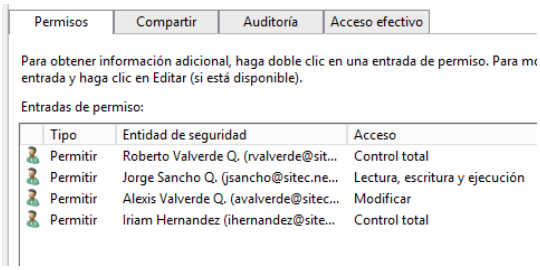
- Se utilizarán cuentas separadas para fines de administración, en lugar de que los usuarios utilicen sus cuentas personales con privilegios elevados, para evitar la mezcla de actividades personales y administrativas, gestionado por el departamento de tecnología de la información.

Se realizan revisiones periódicas mínimo cada 3 meses de los derechos de acceso privilegiados para garantizar que solo aquellos usuarios que realmente necesitan esos privilegios sigan teniendo acceso, incluye la validación de las cuentas con privilegios elevados y la revocación de aquellos privilegios que ya no sean necesarios.

- Las revisiones de acceso son documentadas y se recomienda llevarse a cabo al menos una vez al año o cuando se produzcan cambios significativos en los roles o responsabilidades de los usuarios, por el departamento de tecnología de la información.

Sitec Seguridad utiliza controles de acceso basados en roles (RBAC) para asignar y administrar los privilegios de acceso privilegiados, los usuarios recibirán acceso a recursos específicos según sus roles en la empresa, y cada rol tendrá permisos establecidos que limitan las acciones que pueden llevar a cabo.

- Los privilegios se ajustan a las necesidades operativas de cada rol, sin conceder más privilegios de los estrictamente necesarios, por el departamento de tecnología de la información.



Se aplican mecanismos robustos de autenticación para las cuentas con privilegios elevados, como el uso de autenticación multifactor (MFA) siempre que sea posible, para evitar el acceso no autorizado a los sistemas críticos, controlados por el departamento de tecnología de la información.

- Las contraseñas de las cuentas privilegiadas deben cumplir con estándares rigurosos de complejidad y longitud, y se deben cambiar regularmente, como mínimo cada 90 días.

Los derechos de acceso privilegiados deben ser revocados de inmediato cuando un usuario cambie de rol, abandone la empresa o ya no necesite esos privilegios, la revocación debe ser procesada sin demora para minimizar los riesgos de accesos no autorizados, por el departamento de tecnología de la información.

- Se implementa procesos automáticos o manuales para la desactivación de cuentas de usuarios que no se utilicen, y también para aquellos que se encuentren en desuso por largos períodos, como la revisión cada 3 meses o cada vez que ocurra un cambio de rol, inclusión o exclusión de personal.

Cuando se requiera otorgar acceso privilegiado temporal a un usuario (por ejemplo, en situaciones de emergencia o durante proyectos específicos), este acceso debe ser aprobado,

limitado en el tiempo y monitoreado estrechamente, por el departamento de tecnología de la información.

- Las cuentas temporales deben ser configuradas con los privilegios mínimos necesarios y desactivadas una vez que se haya completado la tarea o proyecto.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la empresa. Debido a la importancia de proteger los activos y la información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente. La evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE RESTRICCION DE ACCESO A LA INFORMACIÓN

Ilustración 71 - Política de restricción de acceso a la información

(ISO, s.f.)

INTRODUCCIÓN:

La información es uno de los activos más valiosos de una organización, y su protección frente a accesos no autorizados es esencial para la seguridad y continuidad de las operaciones, la gestión adecuada del acceso a la información ayuda a minimizar riesgos de pérdida de confidencialidad, integridad y disponibilidad de los datos, todo acceso a la información debe ser restringido y controlado para asegurar que solo las personas autorizadas tengan acceso a los recursos necesarios, y que dicho acceso se realice de acuerdo con el principio de "mínimo

privilegio", la política establece las directrices necesarias para la correcta gestión de las restricciones de acceso a la información, alineándose con los requisitos de la norma ISO 27001:2022.

PROPÓSITO:

El propósito de esta política es garantizar que el acceso a la información dentro de la organización esté restringido y controlado de manera adecuada, asegurando que los datos solo sean accesibles por las personas autorizadas, en el momento adecuado y en el contexto adecuado. Esta política busca:

- Definir los controles y principios para la restricción de acceso a la información.
- Garantizar la integridad y confidencialidad de la información dentro de Sitec Seguridad.
- Reducir los riesgos de exposición indebida de la información a usuarios no autorizados.
- Asegurar el cumplimiento de la normativa aplicable en materia de seguridad de la información.

ALCANCE:

Esta política se aplica a todos los empleados, contratistas, proveedores, y terceros que tengan acceso a los sistemas de información, bases de datos, documentos electrónicos o cualquier otro tipo de información que sea propiedad o esté bajo la responsabilidad de Sitec Seguridad, incluye:

- Todos los sistemas informáticos, redes y aplicaciones utilizados por Sitec Seguridad.

- Información almacenada en bases de datos, servidores, y dispositivos terminales.
- Documentos físicos y electrónicos relacionados con los procesos de Sitec Seguridad.
- Cualquier otro tipo de acceso a la información que se gestione dentro de Sitec Seguridad.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Sistema de Gestión de la Seguridad de la Información (SGSI).
- ISO/IEC 27002:2022 – Código de buenas prácticas para la gestión de la seguridad de la información.
- Política de seguridad de la información Código A.5.1.01.2025.
- Política general de Información de autenticación A5.17.01.2025.
- Política de Concientización, educación y capacitación sobre seguridad de la información A6.3.01.2025.
- Política de seguridad de redes A8.20.01.2025.

CONTENIDO DE LA POLÍTICA:

Acceso basado en el principio de mínimo privilegio, los usuarios tienen acceso únicamente a la información y recursos que necesiten para cumplir con sus responsabilidades laborales, y no más, este acceso debe ser otorgado y revocado de acuerdo con el principio de "mínimo privilegio".

- El acceso a la información es gestionado en función de los roles y responsabilidades de cada usuario dentro de Sitec Seguridad, se debe establecer una matriz de control de acceso que defina qué roles tienen acceso a qué tipos de información (GPO), lo anterior gestionado por el departamento de tecnologías de la información.

Los accesos a los sistemas requieren de autenticación segura, utilizando mecanismos como contraseñas robustas, autenticación multifactorial (MFA) y otras tecnologías de validación, según corresponda y solo permitirán el acceso a aquellos usuarios que se encuentren debidamente autenticados.

El acceso a la información es revocado de manera inmediata cuando ya no sea necesario, como cuando un empleado cambia de puesto o termina su relación laboral con Sitec Seguridad.

- Se debe realizar una revisión periódica de los derechos de acceso de los usuarios para asegurar que los accesos sigan siendo adecuados y que no existan privilegios innecesarios, la revisión debe ser realizada al menos de forma anual o cuando ocurra un cambio de personal en la empresa, lo anterior gestionado por el departamento de tecnologías de la información.
- El acceso a información clasificada como sensible o confidencial está restringido a personal autorizado y basado en justificaciones claras de necesidad, además, se implementa medidas adicionales de seguridad para proteger dicha información, como cifrado o monitorización de accesos, lo anterior gestionado por el departamento de tecnologías de la información.

El acceso a sistemas críticos (bases de datos, servidores, redes, etc.) es estrictamente controlado y limitado a personal que requiera acceso para realizar sus funciones laborales, los accesos a estos sistemas están sujetos a políticas de seguridad adicionales, como registros de auditoría detallados y autenticación multifactorial.

- Todos los accesos a los sistemas críticos deben ser registrados y monitoreados para detectar cualquier acceso no autorizado o inusual, estos registros deben ser revisados regularmente y se deben tomar medidas ante cualquier anomalía detectada, lo anterior gestionado por el departamento de tecnologías de la información.
- Los dispositivos móviles utilizados para acceder a la información de la organización deben estar protegidos con medidas de seguridad adecuadas, como cifrado, autenticación robusta y control de acceso remoto, además, deben ser gestionados bajo políticas de gestión de dispositivos móviles (MDM) que permitan monitorear y asegurar la información, lo anterior gestionado por el departamento de tecnologías de la información.
- El acceso a la información desde dispositivos externos, como dispositivos USB o almacenamiento en la nube, es controlado y supervisado, lo anterior gestionado por el departamento de tecnologías de la información.

Sitec Seguridad a través del departamento de tecnología de la información y talento humano realiza entrenamientos cortos de refrescamiento (por ejemplo, videos, charlas, flyers, entre otros) sobre temas claves, emergentes o actualizaciones.

- Flyer ubicados en áreas estratégicas de la empresa (comedor, servicios sanitarios, recepción, entre otros.).

- Capacitaciones y /o reforzamiento cada 3 a 6 meses o cuando se produzcan cambios significativos en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización. Debido a la importancia de proteger los activos y la información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente. La evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE AUTENTICACIÓN SEGURA

Ilustración 72 - Política de autenticación segura

(TECNOGEEK, s.f.)

INTRODUCCIÓN:

La autenticación segura es un componente clave en la protección de los sistemas de información y los recursos tecnológicos de la empresa, el acceso no autorizado a sistemas y aplicaciones puede exponer información confidencial, comprometer la integridad de los procesos operativos y poner en riesgo la seguridad de Sitec Seguridad, para mitigar estos riesgos, es crucial implementar métodos de autenticación robustos y efectivos, garantizando que solo los usuarios legítimos y autorizados puedan acceder a los recursos protegidos, la política está alineada con el control A.8.5 de la norma ISO/IEC 27001:2022, que establece los requisitos y directrices para asegurar que la autenticación de usuarios se realice de forma segura y confiable.

PROPÓSITO:

El propósito de esta política es definir los procedimientos, principios y controles necesarios para garantizar que la autenticación de usuarios en los sistemas y aplicaciones de la empresa se realice de manera segura, lo que incluye el uso de mecanismos adecuados para verificar la identidad de los usuarios, proteger las credenciales de acceso y minimizar el riesgo de acceso no autorizado o fraude.

La autenticación segura es fundamental para proteger los sistemas y datos sensibles de la empresa y la política establece un marco claro para la implementación de mecanismos robustos de autenticación que aseguren que solo los usuarios autorizados puedan acceder a los recursos críticos de la empresa.

El cumplimiento con esta política es esencial para mitigar los riesgos de seguridad asociados con accesos no autorizados, robo de credenciales y fraudes, y para garantizar la integridad de la información manejada por Sitec Seguridad.

ALCANCE:

Esta política aplica a todos los sistemas de información, aplicaciones, plataformas de red, bases de datos y servicios utilizados dentro de Sitec Seguridad que requieran autenticación de usuarios para acceder a información sensible o recursos críticos, también cubre todos los usuarios que acceden a estos sistemas, ya sean colaboradores, contratistas, proveedores o cualquier tercero que requiera acceso a los recursos tecnológicos de la empresa.

La política cubre:

- Sistemas de acceso a redes internas.
- Aplicaciones empresariales y plataformas de software.

- Dispositivos móviles y computadoras de escritorio.
- Servicios en la nube utilizados por la empresa.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Control A.8.5 (Autenticación segura).
- Política de seguridad de la información Código A.5.1.24.01.2025.
- Política de derechos de acceso privilegiados Código: A8.2.24.01.2025.
- Política de construcción de contraseñas Código: A5.17.01.2025.

CONTENIDO DE LA POLÍTICA:

Todos los sistemas que manejan información sensible o acceso a recursos críticos deben implementar mecanismos de autenticación robustos, como el uso de contraseñas fuertes y, cuando sea posible, autenticación multifactor (MFA), lo anterior gestionado por el departamento de tecnologías de la información.

Las contraseñas deben cumplir con los requisitos de complejidad establecidos por la empresa (mínimo de 12 caracteres, inclusión de mayúsculas, minúsculas, números y caracteres especiales), la anterior de acuerdo a la política de información de autenticación.

Se debe implementar autenticación basada en algo que el usuario sabe (contraseña), algo que el usuario tiene (token, dispositivo de seguridad) y algo que el usuario es (biometría), en combinación cuando sea necesario.

La autenticación multifactor (MFA) debe ser obligatoria para el acceso a sistemas sensibles, aplicaciones críticas o redes internas, así como para el acceso remoto a la empresa.

Los factores de MFA deben incluir al menos dos de los siguientes:

- Algo que el usuario sabe (contraseña o PIN)
- Algo que el usuario tiene (token físico o aplicación de autenticación)
- Algo que el usuario es (reconocimiento biométrico)

El uso de MFA debe extenderse también a la administración de cuentas privilegiadas, como las cuentas de administrador o superusuario.

Las contraseñas deben ser cambiadas regularmente, al menos cada 90 días, y nunca deben reutilizarse entre diferentes sistemas o plataformas.

Los usuarios no deben compartir sus contraseñas con otros, y las contraseñas no deben ser almacenadas de manera insegura, se recomienda el uso de gestores de contraseñas seguros en lugar de guardar contraseñas en papel o en archivos no protegidos.

- Las contraseñas predeterminadas para cualquier sistema o dispositivo deben ser modificadas antes de ponerlos en producción.

Las credenciales de autenticación deben ser cifradas tanto en tránsito (cuando se transmiten por la red) como en reposo (cuando se almacenan en bases de datos o archivos).

- El acceso a las credenciales debe estar restringido a personal autorizado y debe ser gestionado de acuerdo con la política de control de accesos de la empresa.

Cualquier acceso remoto a los sistemas internos de la empresa debe estar sujeto a mecanismos de autenticación segura, como MFA y gestionado por el departamento de tecnologías de la información.

- Los accesos remotos deben ser monitorizados y registrados para garantizar que cualquier actividad sospechosa sea identificada y gestionada de manera adecuada, lo anterior gestionado por el departamento de tecnologías de la información.

Se deben realizar revisiones periódicas de las cuentas de usuario y sus privilegios de acceso o cuando un usuario cambie de rol o abandone la empresa, sus credenciales de acceso deben ser revocadas de manera inmediata.

- Las cuentas inactivas durante un período de tiempo prolongado deben ser desactivadas para evitar el riesgo de acceso no autorizado, lo anterior gestionado por el departamento de tecnologías de la información.

Los sistemas deben implementar medidas de control para prevenir ataques de fuerza bruta, como limitar el número de intentos fallidos de autenticación y activar un bloqueo temporal de la cuenta después de varios intentos fallidos.

- Los intentos de acceso no autorizado deben ser registrados y revisados para detectar patrones inusuales que puedan indicar un intento de intrusión, lo anterior gestionado por el departamento de tecnologías de la información.

El acceso a cuentas con privilegios elevados (como administradores del sistema o súper usuarios) debe requerir una autenticación aún más robusta, preferiblemente con autenticación multifactor.

- Las cuentas privilegiadas deben ser auditadas regularmente, los accesos realizados con estas cuentas deben ser registrados de forma detallada para su posterior análisis en caso de incidencias, lo anterior gestionado por el departamento de tecnologías de la información.

Se llevarán a cabo auditorías periódicas para garantizar que la autenticación de usuarios se realice conforme a esta política y a los estándares de seguridad establecidos.

- Las auditorías deben incluir la verificación de la implementación de MFA, la correcta gestión de contraseñas y la efectividad de los controles de acceso, lo anterior gestionado por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la empresa. Debido a la importancia de proteger los activos y la información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente. La evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE PROTECCIÓN CONTRA MALWARE

Ilustración 73 - Política de protección contra malware

(CYBERSECURITY360, 2022)

INTRODUCCIÓN:

La creciente dependencia de las tecnologías de la información y comunicación (TIC) en las organizaciones ha generado un aumento en los riesgos asociados a la ciberseguridad, siendo el malware una de las amenazas más graves, el malware (software malicioso) abarca una

variedad de programas diseñados para dañar, interrumpir o acceder de manera no autorizada a sistemas informáticos y redes, por lo que esta política tiene como objetivo establecer los principios y controles necesarios para proteger los activos de la organización frente a este tipo de amenazas, garantizando la integridad, disponibilidad y confidencialidad de la información y se basa en el control A.8.7 de la norma ISO/IEC 27001:2022, que establece las directrices para la protección de malware dentro la organización.

PROPÓSITO:

El propósito de esta política es establecer directrices claras para prevenir, detectar y responder a incidentes de malware en la infraestructura de TI de Sitec Seguridad, incluye la implementación de medidas de seguridad que aseguren la protección de todos los sistemas, redes, dispositivos y aplicaciones frente a la instalación y propagación de malware.

La protección contra el malware es un componente esencial en la estrategia global de seguridad de la información de Sitec Seguridad y la implementación efectiva de esta política garantizará que se tomen medidas proactivas, como reactivas para prevenir y mitigar los riesgos asociados al malware, protegiendo así los activos de la organización y asegurando la continuidad de las operaciones.

ALCANCE:

Esta política es aplicable a todos los sistemas de información, usuarios, dispositivos, redes y aplicaciones que se encuentran dentro del perímetro de seguridad de Sitec Seguridad, incluye tanto los entornos de trabajo como los dispositivos personales utilizados por los empleados que

acceden a los recursos corporativos, además, la política debe ser seguida por todo el personal, contratistas y terceros que tengan acceso a los sistemas de información de la empresa.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Sistema de gestión de seguridad de la información (SGSI), específicamente el Anexo A, 8.7 (Protección contra malware).
- Política de seguridad de la información Código A.5.1.24.01.2025

CONTENIDO DE LA POLÍTICA:

Las siguientes tareas serán realizadas por el departamento de tecnología de la información para la prevención de Malware:

- Instalar y mantener actualizados los programas antivirus y antimalware en todos los dispositivos de la empresa.
- Configurar sistemas de protección en tiempo real (firewalls, sistemas de detección de intrusos) para bloquear la entrada de malware.
- Deshabilitar el uso de dispositivos USB no autorizados o controlar estrictamente el acceso a dispositivos de almacenamiento externos.
- Restringir la instalación de software no autorizado y ejecutar solo aplicaciones aprobadas.

- Utilizar herramientas de filtrado de contenido web para prevenir la descarga de malware a través de Internet.

Implementar sistemas de monitoreo y escaneo periódico para detectar la presencia de malware en los sistemas de información, lo anterior gestionado por el departamento de tecnologías de la información.

Mantener actualizadas las bases de datos de firmas de antivirus para detectar las variantes más recientes de malware, lo anterior gestionado por el departamento de tecnologías de la información.

Realizar auditorías regulares en los sistemas para identificar actividades sospechosas que puedan indicar una infección de malware, lo anterior gestionado por el departamento de tecnologías de la información.

Se establece un protocolo claro para la respuesta ante incidentes de malware, que incluye la identificación, contención y eliminación del malware de los sistemas afectados.

- Aislar rápidamente los sistemas infectados para evitar la propagación del malware a otros dispositivos.
- Documentar cada incidente para realizar un análisis post-incidente y mejorar las medidas de seguridad.
- Notificar de manera oportuna a las partes interesadas, incluyendo a la alta dirección y, en su caso, a las autoridades pertinentes.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Proveer formación periódica a todos los usuarios sobre las amenazas del malware y las buenas prácticas para evitar la instalación de software malicioso (p. ej., no abrir correos electrónicos o enlaces desconocidos), lo anterior gestionado por el departamento de tecnologías de la información y talento humano.

Actualizar los sistemas operativos, aplicaciones y herramientas de seguridad con regularidad para corregir vulnerabilidades conocidas que podrían ser explotadas por malware, lo anterior gestionado por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para los colaboradores del departamento de TI de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente,

la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE COPIA DE SEGURIDAD DE LA INFORMACIÓN

Ilustración 74 - Política de copia de seguridad de la información

(explicados, 2024)

INTRODUCCIÓN:

En un entorno digital cada vez más dependiente de la tecnología, la protección de los datos es esencial para asegurar la continuidad de las operaciones, la preservación de la confidencialidad e integridad de la información, y el cumplimiento con las normativas legales y regulatorias, las copias de seguridad de la información son una medida clave para garantizar la recuperación de datos críticos en caso de incidentes como fallos del sistema, desastres naturales o ciberataques, la política establece las directrices y procedimientos necesarios para la creación,

almacenamiento y recuperación de copias de seguridad, con el fin de minimizar los impactos de la pérdida de información., se basa en el control A.8.13 de la norma ISO/IEC 27001:2022, que establece las directrices para las copias de seguridad de la información dentro la organización.

PROPÓSITO:

El propósito de esta política es definir el enfoque organizacional para la creación y gestión de copias de seguridad de la información, asegurando que los datos críticos estén protegidos contra pérdidas, daños o accesos no autorizados y tiene como objetivo garantizar que las copias de seguridad sean realizadas de manera regular, que sean almacenadas de forma segura, y que se pueda recuperar la información de manera eficiente y dentro de los plazos establecidos, en caso de ser necesario.

ALCANCE:

Esta política es aplicable a toda la información gestionada por la organización, tanto en formato digital como en otros tipos de almacenamiento, y a todos los sistemas, aplicaciones, bases de datos, servidores y dispositivos de almacenamiento utilizados, no se limita a la información almacenada en servidores locales, en la nube, en dispositivos móviles y en cualquier otro entorno de almacenamiento que sea parte de la infraestructura de TI de Sitec Seguridad, también abarca a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información de la organización..

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Sistema de gestión de seguridad de la información (SGSI), Anexo A.8.13 – Copia de seguridad de la información.
- Política de seguridad de la información Código A.5.1.01.2025
- Política general de medios de almacenamiento Código: A7.10.01.2025

CONTENIDO DE LA POLÍTICA:

Las copias de seguridad deben realizarse de forma regular y periódica, con una frecuencia adecuada según la criticidad de los datos, las copias de seguridad completas deben realizarse al menos de forma semanal, mientras que las copias incrementales o diferenciales deben realizarse diariamente.

- Los datos críticos y sensibles deben ser objeto de copias de seguridad con mayor frecuencia y en intervalos que garanticen la mínima pérdida de información en caso de un incidente, lo anterior gestionado por el departamento de tecnologías de la información.

Copia de seguridad completa se realizará al menos una vez por semana, respaldando todos los datos y sistemas definidos como críticos para la operación de la organización, lo anterior gestionado por el departamento de tecnologías de la información.

Copia de seguridad incremental se realizará diariamente para registrar únicamente los cambios realizados desde la última copia de seguridad completa o incremental, lo anterior gestionado por el departamento de tecnologías de la información.

Copia de seguridad diferencial en caso de que se utilice este enfoque, se realizará diariamente para respaldar los cambios realizados desde la última copia de seguridad completa, lo anterior gestionado por el departamento de tecnologías de la información.

Las copias de seguridad deben almacenarse en ubicaciones seguras, que pueden incluir almacenamiento en la nube, servidores remotos o dispositivos físicos cifrados.

- Las copias de seguridad deben estar protegidas contra accesos no autorizados mediante controles de seguridad, como el cifrado de datos, el uso de contraseñas robustas y la implementación de autenticación multifactor, lo anterior gestionado por el departamento de tecnologías de la información.

Las copias de seguridad deben verificarse periódicamente para asegurar que los datos se han respaldado correctamente y que las copias pueden ser restauradas con éxito, incluye la validación de la integridad de las copias y la prueba de la capacidad de restauración de los datos.

- Las pruebas de restauración deben llevarse a cabo de forma regular, al menos una vez al año, y deben incluir la restauración de datos completos en un entorno de prueba, lo anterior gestionado por el departamento de tecnologías de la información.

Cuando se utilicen servicios de almacenamiento en la nube o servidores remotos para las copias de seguridad, estos deben cumplir con los mismos requisitos de seguridad que los sistemas locales, la implementación de cifrado de datos en reposo, en tránsito y la realización de auditorías de seguridad para garantizar que las copias de seguridad no sean vulnerables a accesos no autorizados, lo anterior gestionado por el departamento de tecnologías de la información.

Las copias de seguridad deben ser retenidas durante un período determinado, basado en los requisitos legales, regulatorios y operativos, las copias de seguridad completas se deben retener por un mínimo de 6 meses, mientras que las copias de seguridad incrementales pueden ser retenidas por un período más corto.

- Las políticas de retención de copias de seguridad deben ser revisadas periódicamente para garantizar que se ajusten a los requisitos y necesidades de la organización, lo anterior gestionado por el departamento de tecnologías de la información y departamento administrativo.

La empresa debe tener procedimientos documentados y probados para la recuperación de los datos a partir de las copias de seguridad en caso de pérdida de información, corrupción de datos o un ataque de ransomware.

- La restauración de datos debe ser realizada de manera eficiente, con plazos de recuperación predefinidos para asegurar la mínima interrupción de las operaciones, lo anterior gestionado por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

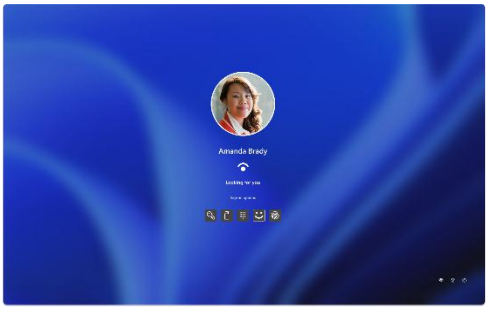
ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE INICIO DE SESIÓN

Ilustración 75 - Política de inicio de sesión



(Microsoft, Acceso a cuentas de usuario en Windows, s.f.)

INTRODUCCIÓN:

El inicio de sesión es uno de los puntos críticos en la gestión de accesos a los sistemas de información, la autenticación adecuada en el momento del inicio de sesión asegura que solo los usuarios legítimos puedan acceder a los recursos de la empresa, previniendo el acceso no autorizado y la posible exposición de información sensible, a través de controles adecuados en el proceso de inicio de sesión se protege la confidencialidad, integridad y disponibilidad de los sistemas de Sitec Seguridad, la política está basada en el control A.8.15 de la norma ISO/IEC 27001:2022, que establece los principios y medidas de seguridad que deben aplicarse durante el proceso de inicio de sesión para garantizar que se minimicen los riesgos asociados al acceso no autorizado.

PROPÓSITO:

El propósito de esta política es establecer los lineamientos necesarios para garantizar que el inicio de sesión a los sistemas de la empresa se realice de manera segura, asegurando la autenticación adecuada de los usuarios, la protección de las credenciales de acceso y la monitorización del acceso a los recursos informáticos, con la implementación de mecanismos de control y la gestión de los accesos a los sistemas, tanto de forma local como remota.

El inicio de sesión es una de las primeras líneas de defensa en la protección de los recursos de la empresa y establece las directrices necesarias para garantizar que los procesos de autenticación durante el inicio de sesión sean seguros, controlados y monitoreados adecuadamente.

Cumplir con esta política ayudará a minimizar los riesgos de acceso no autorizado y protegerá la confidencialidad, integridad y disponibilidad de la información y los sistemas de la empresa.

ALCANCE:

Esta política aplica a todos los sistemas de información, plataformas de software, aplicaciones, redes y dispositivos de la empresa que requieran un proceso de inicio de sesión para acceder a sus recursos, incluye, pero no se limita a:

- Sistemas operativos y aplicaciones empresariales
- Plataformas de gestión de bases de datos
- Dispositivos de red como switches, routers y firewalls
- Servicios en la nube y sistemas de acceso remoto
- Dispositivos móviles, computadoras de escritorio y portátiles utilizados por la empresa

La política aplica a todos los usuarios que accedan a estos sistemas, incluyendo colaboradores, contratistas, proveedores y otros terceros autorizados.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Control A.8.15 (Inicio de sesión).
- Política de seguridad de la información Código A.5.1.01.2025.

- Política de información de autenticación A5.17.01.2025.
- Política de autenticación segura Código: A8.5.01.2025.
- Procedimiento de Autenticación Multifactor (MFA)

CONTENIDO DE LA POLÍTICA:

Todo acceso a sistemas y aplicaciones debe requerir una autenticación de usuario mediante un nombre de usuario y contraseña válidos, este proceso de inicio de sesión debe garantizar que el usuario sea el legítimo propietario de la cuenta.

- Se debe implementar la autenticación multifactor (MFA) para el inicio de sesión en sistemas y aplicaciones que manejen información sensible o que sean considerados de alto riesgo.
- Las contraseñas utilizadas en el proceso de inicio de sesión deben cumplir con los requisitos de complejidad establecidos por la empresa, tales como una longitud mínima de 12 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Para proteger los sistemas contra ataques de fuerza bruta y otros intentos de acceso no autorizado, se debe establecer un límite de intentos fallidos de inicio de sesión, después de un número determinado de intentos fallidos (por ejemplo, 5 intentos), la cuenta debe ser bloqueada temporalmente y se debe activar una alerta de seguridad.

- Los intentos fallidos deben ser registrados y monitoreados para detectar patrones inusuales que puedan indicar intentos de intrusión.

- Lo anterior gestionado por el departamento de tecnologías de la información.

Todos los inicios de sesión deben ser registrados y auditados cada 3 meses por el departamento de tecnología de la información para garantizar que cualquier acceso a los sistemas sea legítimo y autorizado, los registros deben incluir la identificación del usuario, la fecha y hora del inicio de sesión, la dirección IP desde la que se realizó el acceso y el sistema o recurso al que se accedió.

- Los registros de inicio de sesión deben ser almacenados de forma segura y mantenerse durante un período adecuado, conforme a las políticas de retención de datos de la empresa.

El inicio de sesión en sistemas que contienen información confidencial o que tienen acceso a recursos críticos debe requerir la autenticación multifactor (MFA) con la combinación de al menos dos de los siguientes factores:

- Algo que el usuario sabe (contraseña o PIN)
- Algo que el usuario tiene (token, dispositivo de autenticación o aplicación de autenticación)
- Algo que el usuario es (reconocimiento biométrico)

MFA debe ser obligatorio para accesos remotos, aplicaciones de gestión de sistemas y plataformas que almacenen datos sensibles, lo anterior gestionado por el departamento de tecnologías de la información.

Las contraseñas deben ser almacenadas de forma segura utilizando algoritmos de cifrado adecuados, no deben ser almacenadas en texto claro ni en formatos inseguros.

- El acceso a las credenciales de inicio de sesión debe estar restringido a personal autorizado y debe ser gestionado conforme a las políticas de control de accesos de la empresa, lo anterior gestionado por el departamento de tecnologías de la información.

El inicio de sesión remoto a sistemas de la empresa debe estar restringido a usuarios autorizados y debe contar con controles adicionales de seguridad, como VPN (Red Privada Virtual) y MFA.

- Todo acceso remoto debe ser monitoreado de forma continua y los registros deben ser auditados cada 3 meses para identificar accesos no autorizados o comportamientos anómalos, lo anterior gestionado por el departamento de tecnologías de la información.

Los sistemas deben implementar un tiempo de espera de sesión para desconectar automáticamente a los usuarios después de un período de inactividad

- El tiempo de inactividad permitido debe ser determinado según la sensibilidad de los recursos y el contexto de la empresa (por ejemplo, 15 minutos de inactividad para accesos críticos).
- Los usuarios deben ser notificados de la desconexión y se les debe dar la opción de volver a autenticarse si lo desean.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Si un usuario abandona la empresa, cambia de rol o pierde la necesidad de acceso a ciertos sistemas, sus derechos de acceso deben ser revocados de manera inmediata para prevenir accesos no autorizados.

- Las credenciales de usuario no deben permanecer activas una vez que ya no se necesiten, y cualquier cuenta inactiva durante un largo período debe ser desactivada.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la empresa. Debido a la importancia de proteger los activos y la información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente. La evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad

del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

POLÍTICA GENERAL DE SEGURIDAD DE REDES

Ilustración 76 - Política de seguridad de redes

(DELTAPROTECT, 2024)

INTRODUCCIÓN:

Las redes de comunicación son fundamentales para las operaciones diarias de cualquier empresa moderna, ya que permiten la transferencia de información y el acceso a recursos críticos, sin embargo, las redes también son un punto vulnerable, ya que un acceso no autorizado o una vulnerabilidad en ellas puede comprometer la seguridad de los sistemas de información.

La implementación de una política de seguridad de redes robusta es esencial para proteger los activos de Sitec Seguridad, garantizando la integridad, confidencialidad y disponibilidad de los datos que se transmiten a través de ellas, la política se basa en el control

A.8.20 de la norma ISO/IEC 27001:2022, que establece las directrices para asegurar la protección de las redes y las comunicaciones de la empresa.

PROPÓSITO:

El propósito de esta política es definir las medidas y procedimientos de seguridad necesarios para proteger las redes de comunicación de la empresa contra accesos no autorizados, ataques cibernéticos y otros riesgos que puedan comprometer la seguridad de la información.

Esto incluye la protección de los sistemas de red, la infraestructura de comunicaciones y los servicios relacionados, garantizando la integridad de las redes y el cumplimiento con las normativas de seguridad.

La protección de las redes es crucial para salvaguardar la información y los recursos de la empresa, por lo que se establece un marco integral de medidas de seguridad para proteger las redes y las comunicaciones internas y externas, así como su implementación eficaz contribuirá a reducir significativamente los riesgos de acceso no autorizado, vulnerabilidades y amenazas externas, garantizando la seguridad de los datos y los sistemas.

La empresa debe asegurar que todas las directrices contenidas en esta política se cumplan rigurosamente, protegiendo así la integridad y la confiabilidad de sus redes.

ALCANCE:

Esta política se aplica a todos los sistemas de red y equipos de comunicación utilizados por la empresa, tanto en sus instalaciones físicas como en servicios en la nube, aplicaciones remotas y redes externas, el alcance de la misma incluye, pero no se limita a:

- Redes locales (LAN) e inalámbricas (Wi-Fi).
- Redes de área amplia (WAN).
- Sistemas de comunicaciones móviles y conexiones remotas.
- Dispositivos de red (routers, switches, AP, etc.).
- Servicios de comunicación en la nube y sistemas de intercambio de información.
- Plataformas de acceso remoto y conexiones VPN.

La política aplica a todos los colaboradores, contratistas y terceros que tengan acceso a las redes de la empresa, así como a cualquier equipo, dispositivo o sistema que esté conectado a dichas redes.

DOCUMENTOS APLICABLES:

Para garantizar la correcta implementación y aplicación de esta política, se deben consultar y aplicar los siguientes documentos:

- ISO/IEC 27001:2022 – Control A.8.20 (Seguridad de redes).
- Política de seguridad de la información Código A.5.1.01.2025.
- Política de inventario de información y otros activos asociados Código: A5.9.01.2025.
- Política de seguridad de oficina e instalaciones Código: A7.3.01.2025.
- Procedimiento de Autenticación Multifactor (MFA).

CONTENIDO DE LA POLÍTICA:

La infraestructura de red debe ser diseñada, implementada y mantenida de acuerdo con los principios de seguridad, asegurando que todas las conexiones de red sean seguras y que se implementen mecanismos de protección adecuados para prevenir accesos no autorizados.

- Los dispositivos de red (routers, switches, AP, etc.) deben estar configurados para minimizar los riesgos de intrusión, y debe asegurarse que las configuraciones predeterminadas sean cambiadas antes de poner en funcionamiento cualquier dispositivo nuevo.
- Se deben emplear tecnologías de segmentación de red para aislar los recursos más sensibles, garantizando que el acceso a las redes críticas esté restringido y que se minimicen los impactos de posibles incidentes.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Se debe implementar un control de acceso basado en la autenticación y autorización de los usuarios para restringir el acceso a las redes y los recursos según sea necesario, incluyendo el uso de redes privadas virtuales (VPN) para el acceso remoto y el establecimiento de políticas claras de acceso y privilegios para los usuarios.

- Las redes de la empresa deben contar con mecanismos de autenticación multifactor (MFA) cuando sea posible, especialmente para accesos remotos o administradores de sistemas.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Se debe implementar una monitorización continua de la red para detectar actividades sospechosas y posibles amenazas, incluido el uso de sistemas de detección y prevención de intrusiones (IDS/IPS), firewalls, y herramientas de monitoreo de tráfico.

- Los registros de acceso y actividades en la red deben ser recolectados, almacenados y auditados regularmente cada 3 meses para detectar posibles incidentes de seguridad, deben incluir información sobre la identidad del usuario, la dirección IP de origen, los recursos a los que se accedió, y los resultados de las transacciones.
- Las auditorías deben incluir una revisión periódica cada 3 meses de la configuración de dispositivos de red para garantizar que cumplan con las políticas de seguridad establecidas.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Todas las comunicaciones de datos a través de las redes deben ser cifradas para garantizar la confidencialidad e integridad de la información, él mismo debe ser implementado tanto en la transmisión de datos (por ejemplo, mediante protocolos TLS/SSL) como en el almacenamiento de datos sensibles.

- Las comunicaciones en redes públicas o no confiables deben ser protegidas utilizando tecnologías de cifrado de extremo a extremo para prevenir la interceptación de datos.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Se deben implementar medidas de seguridad para proteger la red contra amenazas externas, como ataques de denegación de servicio (DoS), virus, malware, y accesos no autorizados, lo que incluye la implementación de firewalls, sistemas de detección de intrusos, y la segmentación de la red para limitar el acceso no autorizado.

- Las conexiones a Internet deben ser filtradas y controladas para evitar que el tráfico malicioso entre a la red interna, bloqueando protocolos o puertos no utilizados, así como aplicar políticas de seguridad para todo el tráfico entrante y saliente.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Las redes inalámbricas deben estar protegidas con cifrado robusto (como WPA3) y deben requerir autenticación para el acceso, no debe permitirse el acceso no autorizado a las redes Wi-Fi internas.

- Se deben emplear controles de acceso específicos para las redes inalámbricas, como la autenticación por MAC address o mediante sistemas de autenticación centralizados (802.1X).
- Lo anterior gestionado por el departamento de tecnologías de la información.

Se deben realizar evaluaciones regulares de seguridad y pruebas de penetración para identificar y corregir vulnerabilidades en la infraestructura de red y los dispositivos asociados.

- Todos los dispositivos de red deben contar con actualizaciones y parches de seguridad aplicados de manera oportuna para mitigar las vulnerabilidades conocidas y reducir el riesgo de explotación.

- Lo anterior gestionado por el departamento de tecnologías de la información.

El acceso remoto a la red debe ser gestionado de manera segura mediante el uso de VPNs, autenticación multi factor, y otros controles que aseguren que solo los usuarios autorizados puedan acceder a la infraestructura de la empresa.

- Las conexiones remotas deben estar restringidas a horarios y períodos específicos, y se debe realizar un monitoreo adicional de las conexiones remotas para detectar accesos sospechosos.
- Lo anterior gestionado por el departamento de tecnologías de la información.

Esta política será revisada **al menos una vez al año**, **complementada con revisiones adicionales cada vez que se produzcan cambios significativos** en la infraestructura, procesos, amenazas o en el contexto de negocio de la organización por el departamento de tecnologías de la información.

El cumplimiento de esta política es obligatorio para todos los colaboradores de la empresa Sitec Seguridad y se tomará en cuenta en la evaluación del desempeño de los mismos.

ACCIONES DISCIPLINARIAS:

El incumplimiento de esta política puede generar consecuencias graves para la seguridad de la organización, debido a la importancia de proteger los activos e información sensible, cualquier violación será tratada con seriedad y dará lugar a medidas disciplinarias, que serán aplicadas según la naturaleza de la infracción.

Las sanciones podrán incluir desde advertencias formales y la suspensión de privilegios de acceso, hasta la terminación de la relación laboral, dependiendo de la gravedad del incidente, la evaluación y determinación de las acciones disciplinarias pertinentes serán responsabilidad del departamento de Talento Humano, quien tomará las decisiones en función de los hechos y las políticas internas establecidas.

Conclusiones

Como punto de partida, se llevó a cabo un diagnóstico detallado de las prácticas utilizadas por SITEC Seguridad en la gestión de riesgos de tecnologías de la información, el análisis realizado a las practicas actuales de la gestión de riesgos de TI en SITEC Seguridad, reflejo que existen aspectos positivos, así como áreas susceptibles de mejora en los procesos y protocolos de seguridad de la información, los cuales fueron desarrollados en el capítulo cinco, el diagnóstico realizado en el capítulo cuatro ha permitido comprender la estructura de gestión de TI en uso por parte de Sitec Seguridad, destacando la necesidad de alinear las estrategias de seguridad con los estándares y mejores prácticas establecidos en el marco COBIT 2019, el diagnóstico incluye:

- La revisión de políticas existentes de seguridad.
- La evaluación del nivel de madurez en la implementación de controles.
- El análisis de herramientas tecnológicas actualmente en uso.
- La identificación de brechas de cumplimiento con normas reconocidas.

Aunque la empresa ha implementado ciertos controles, se ha identificado un margen para optimizar y formalizar los procedimientos de gestión de riesgos, así como para fortalecer la capacitación y la sensibilización del personal debido a los resultados obtenidos en el diagnóstico de percepción, por lo que se recomienda continuar desarrollando el manual interno de gestión de TI que contemple las mejores prácticas y protocolos de seguridad, conforme a las directrices de COBIT 2019, lo que permitirá garantizar un enfoque más estructurado y efectivo en la protección de la información de Sitec Seguridad.

A partir de los datos recopilados en el diagnóstico, se procedió a un análisis profundo de los protocolos, procesos y controles existentes en SITEC Seguridad, el análisis reveló:

- Un marco de gestión con pocos controles básicos implementados.
- Procesos no estandarizados ni completamente documentados.
- Falta de alineación formal con marcos internacionales como COBIT 2019.
- Brechas en la concienciación del personal respecto a la seguridad de la información.

El objetivo de este análisis fue sentar las bases para el desarrollo de un manual nterno de gestión de TI, que permita utilizar las mejores prácticas y brinde un marco operativo claro y replicable, en línea con los hallazgos del análisis; se propuso el desarrollo de nuevos procedimientos estructurados, tomando como guía el marco de gobierno y gestión de TI COBIT 2019, este marco permite integrar el gobierno corporativo con la gestión operativa, priorizando:

- La identificación y evaluación de riesgos tecnológicos.
- El diseño de controles específicos para minimizar amenazas.
- La definición de roles y responsabilidades en la gestión de seguridad.

- La integración de procesos de monitoreo y mejora continua.

Con base en COBIT 2019, se diseñaron procedimientos que garanticen la trazabilidad, eficacia y escalabilidad en la gestión de TI de SITEC Seguridad, ya que resulta crucial establecer procedimientos claros y bien documentados, acompañados de capacitaciones periódicas para el personal, con el fin de asegurar que todos los empleados comprendan y apliquen adecuadamente las metodologías y medidas de seguridad, lo que contribuirá a reforzar la cultura organizacional en torno a la gestión de riesgos, disminuyendo así las amenazas potenciales y mejorando la seguridad de la información, al reducir las vulnerabilidades en la infraestructura tecnológica.

La fase final de la propuesta contempla la creación de un manual interno de gestión de TI, acompañado de un plan de formación continua que permita una apropiación efectiva del conocimiento por parte del personal de SITEC Seguridad, este proceso incluye:

- Capacitación estructurada sobre las metodologías adoptadas.
- Simulacros de incidentes de seguridad para medir la respuesta organizacional.
- Evaluaciones periódicas de cumplimiento de políticas.
- Actualizaciones constantes del manual conforme evolucione la tecnología y el entorno normativo.

La capacitación periódica es clave para fortalecer la cultura organizacional orientada a la seguridad y para reducir el impacto de errores humanos en la infraestructura tecnológica, el análisis realizado permite concluir que SITEC Seguridad ha tomado medidas iniciales en la gestión de riesgos de TI; sin embargo, aún existen áreas de mejora relevantes, dentro de las que se encuentran:

- La necesidad de alinear de forma integral las estrategias de seguridad con los principios de COBIT 2019.
- La optimización de procedimientos documentados.
- El fortalecimiento de la capacitación y sensibilización del personal, en respuesta a los resultados del diagnóstico de percepción.

Podemos finalizar indicando que la implementación exitosa de estos controles serán determinantes para crear un entorno de TI más seguro y resiliente, alineado con los estándares internacionales y preparado para afrontar los desafíos futuros en la gestión de riesgos, así como continuar con el desarrollo del manual interno de gestión de TI pendientes, mismos controles deben ser basados en COBIT 2019, establecer mecanismos de evaluación continua, pero sobre todo consolidar una cultura de seguridad organizacional desde la dirección hasta el personal operativo.

Recomendaciones

Hemos segmentado las recomendaciones dadas a Sitec Seguridad en varios puntos con el fin de facilitar la interpretación, desarrollo y aplicación de las mismas, las recomendaciones son:

1. Se deben realizar análisis de prácticas, protocolos y procesos de seguridad de la información actuales e implementados, a través de 3 variables claves:
    - Una evaluación exhaustiva la cual permite realizar un análisis detallado de los protocolos y prácticas actuales de seguridad de la información en SITEC Seguridad, identificando fortalezas y debilidades en los controles existentes, el análisis debe

abarcar tanto la seguridad tecnológica como las prácticas organizacionales relacionadas con la gestión de TI, incluyendo:

- La arquitectura de seguridad de red.
- Controles de acceso y autenticación.
- Gestión de contraseñas y dispositivos.
- Procesos de respaldo y recuperación ante desastres.

Dicha evaluación permitirá detectar fortalezas que pueden ser potenciadas y áreas débiles que requieren intervención inmediata.

- La identificación de todas las posibles brechas de seguridad, tales como la falta de monitoreo continuo, políticas de acceso insuficientes o vulnerabilidades en la infraestructura tecnológica, además, debe asegurarse que los protocolos y controles de respuesta ante incidentes sean eficaces y adecuados, pudiendo incluir:
  - Falta de monitoreo en tiempo real.
  - Políticas de acceso mal definidas.
  - Deficiencias en el control de dispositivos móviles.
  - Protocolos de respuesta ante incidentes mal estructurados.

  Este enfoque preventivo ayuda a minimizar riesgos operativos y a fortalecer la infraestructura de TI con medidas correctivas específicas.
- Comparar los procesos actuales con las mejores prácticas recomendadas por marcos internacionales, como COBIT 2019, con lo que se podrá asegurar que los mismos estén alineados con las mejores prácticas en cuanto a gestión de riesgos de TI del mercado, esta comparación les servirá para:
  - Alinear objetivos de TI con los del negocio.

- Establecer responsabilidades claras.
- Priorizar inversiones en seguridad de acuerdo a la criticidad de los activos.

2. Desarrollo de procedimientos y controles pendientes basados en COBIT 2019:
   - Adopción del marco COBIT 2019 para desarrollar procedimientos y controles estandarizados que cubran todos los aspectos críticos de la gestión de riesgos de TI, COBIT 2019 ofrece un enfoque integral para la gestión y gobernanza de TI, cubriendo desde la planificación estratégica hasta la ejecución operativa. incluye:
     - Políticas de seguridad.
     - Gestión de activos y configuraciones.
     - Evaluaciones periódicas de riesgo.
     - Mecanismos de respuesta y recuperación.
   - Procedimientos específicos, claros y detallados para la identificación, evaluación y mitigación de riesgos, basados en las directrices del marco COBIT 2019, los mismos deben incluir la implementación de controles proactivos, así como la definición de métricas para evaluar la efectividad de los controles de seguridad, procedimientos con roles definidos, actividades secuenciales y controles verificables, incluyendo:
     - Identificación de riesgos a nivel de sistema y datos.
     - Métodos de evaluación cuantitativa y cualitativa.
     - Planes de mitigación con plazos y responsables.
   - Integración con la cultura organizacional de Sitec Seguridad para asegurarse que los procedimientos y controles desarrollados sean fáciles de entender e integrar dentro de

la cultura organizacional, estos deben ser prácticos y alineados con los objetivos estratégicos de la empresa.

- Los nuevos controles deben comunicarse de forma accesible.
- Deben vincularse con los objetivos estratégicos del negocio.
- Se debe fomentar la participación activa del personal.

Este enfoque facilita el cambio cultural necesario para la madurez en la gestión de TI.

3. Implementación del Manual mediante capacitación y procedimientos documentados:
   - Desarrollo de un manual interno de TI que contemple las políticas de seguridad aprobadas por la alta dirección, procedimientos operativos y de emergencia, controles y mejores prácticas desarrolladas con roles y responsabilidades en cada capa de SITEC Seguridad, basadas en el marco COBIT 2019, el manual debe estar accesible para todo el personal y servir como una guía detallada para la correcta gestión de la seguridad de la información dentro de Sitec Seguridad.
   - Capacitación continua regular y obligatoria para todo el personal involucrado, las capacitaciones deben enfocarse en las metodologías del manual, son uno de los pilares más importantes junto a las mejores prácticas de seguridad y capacitaciones de las nuevas amenazas tecnológicas, con las cuales el personal comprenda de la importancia de su papel en la gestión de riesgos y la protección de la información, realizando simulacros de incidentes reales, evaluaciones periódicas para verificar el nivel de conocimiento y la constante formación en amenazas emergentes (phishing, malware, ransoware).

- Procedimientos documentados de manera clara y accesible, permitiendo una fácil consulta y actualización de estos, garantizando la consistencia y el cumplimiento de las normas establecidas, además de asegurar y garantizar la trazabilidad, permitir auditorías y facilitar la curva de aprendizaje de nuevos empleados de las actividades de gestión de riesgos.

4. Monitoreo y mejora continua mediante un sistema de auditoría técnica y operativa periódica:
    - Monitoreo de efectividad con mecanismos de evaluación que permitan medir la efectividad de los procedimientos implementados, deben incluir auditorías periódicas y revisiones de seguridad para asegurar que los controles de TI estén funcionando adecuadamente, tiempo medio de respuesta ante incidentes, porcentaje de cumplimiento de políticas y numero de vulnerabilidades críticas mitigadas.
    - Retroalimentación y ajustes que permitan fomentar una cultura de mejora continua mediante la recopilación de retroalimentación de los colaboradores y la adaptación de los procesos según sea necesario, es crucial actualizar el manual de gestión de TI y los procedimientos conforme cambian las amenazas y las tecnologías, así como encuestas de percepción interna, análisis post-implementación y ajustes dinámicos al manual y a los procesos según los cambios tecnológicos y normativos.
    - Cambio o actualización de server con Windows 2012 R2 con el fin de obtener las bondades del fabricante en un entorno de soporte, parches y seguridad adaptada al entorno real de seguridad, su desactualización representa un riesgo crítico, por lo cual

actualizarlo permite contar con soporte de seguridad, compatibilidad con nuevas herramientas y mayor estabilidad operativa.

- Se realizó la recomendación de la colocación correcta de AP la cual fue acogida y aplicada por la compañía, lo que refuerza su compromiso de mejoramiento continuo.
- La compañía aplico un aseguramiento puertas TI tras el análisis expuesto con lo cual se va encaminando a las mejores prácticas planteadas por el marco COBIT 2019
- Se sugiere y se acepta la aplicación de configuración considerada como mínima o básica a los APs de la compañía, reforzando la seguridad de las redes
- Se configura el Active Directory que anteriormente no estaba funcionando correctamente con lo cual muchos controles toman un sentido y aplicación real dentro de la empresa, dando aseguramiento a la información y seguridad de la misma.
- Se implementan aplicativos como Viva Learning de Microsoft para ofrecer capacitaciones y formación al personal.
- Se implementa doble factor de autenticación de Microsoft.

Con estas recomendaciones, SITEC Seguridad podrá fortalecer su gestión de riesgos de TI, alineándose con las mejores prácticas internacionales y mejorando la seguridad de la información a nivel organizacional.

Anexos

Ilustración 77 - Carta Aceptación Sitec Seguridad

San José, 03 de marzo de 2025

UNIVERSIDAD HISPANOAMERICANA
ESCUELA DE INGENIERÍA INFORMÁTICA

A QUIEN CORRESPONDA:

Por medio de la presente, agradecemos y hacemos un reconocimiento al Sr. Roberto Valverde Q. por la elaboración de su tesina bajo el nombre "**DESARROLLO DE UNA PROPUESTA PARA LA IMPLEMENTACIÓN DE PROTOCOLOS BASADOS EN EL MARCO COBIT 2019 PARA LA GESTIÓN DEL DEPARTAMENTO DE TI DE LA EMPRESA SITEC S.A. (SISTEMAS INTEGRADOS DE SEGURIDAD S.A)**".

El desarrollo de su propuesta tiene un valor incalculable para nuestra empresa la cual es una organización PYMES que cuenta con recursos limitados, en un mundo tecnológico su propuesta aborda una problemática actual de la empresa y proporciona herramientas bases para la identificación, tratamiento y prevención de malas prácticas, así como la manera correcta de gestionar la seguridad tecnológica en nuestra compañía.

La propuesta presentada por el Sr. Valverde no solo ofrece una guía, sino que se adapta a la realidad de la empresa aplicando normativas internacionales vigentes, las cuales estamos seguros nos darán un lugar mejor en el mercado aplicando las mismas, estos procedimientos contribuyen de manera significativa a dar un manejo adecuado de la tecnología dentro y fuera de nuestra empresa.

Por ese motivo aceptamos, recibimos y pondremos en acción la propuesta presentada, confiando que su implementación es un recurso valioso para fortalecer nuestra empresa, reiteramos nuestro más sincero agradecimiento al Sr. Roberto Valverde por su esfuerzo, compromiso y contribución inestimable a nuestra empresa.

Atentamente,

JORGE LUIS SANCHO QUESADA (FIRMA)

Firmado digitalmente por JORGE LUIS SANCHO QUESADA (FIRMA)
Fecha: 2025.03.05 07:53:43 -06'00'

Jorge Luis Sancho
Gerente General
Sitec Seguridad

Central Telefónica: (506) 2296-0505
Correos electrónicos: servicioalcliente@sitecseguridad.com - ventas@sitecseguridad.com

Ilustración 78 - Declaración Jurada RVQ

DECLARACIÓN JURADA

Yo Roberto Valverde Quesada, mayor de edad, portador de la cédula de identidad número 1-1087-0929 egresado de la carrera de Ingeniería en Informática de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Bachillerato en Ingenieria Informática, juro solemnemente que mi trabajo de investigación titulado: **DESARROLLO DE UNA PROPUESTA PARA LA IMPLEMENTACIÓN DE PROTOCOLOS BASADOS EN EL MARCO COBIT 2019 PARA LA GESTIÓN DEL DEPARTAMENTO DE TI DE LA EMPRESA SITEC S.A. (SISTEMAS INTEGRADOS DE SEGURIDAD S.A)**, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los _ días del mes de marzo del año dos mil veinticinco.

ROBERTO VALVERDE QUESADA (FIRMA)

Digitally signed by ROBERTO VALVERDE QUESADA (FIRMA)
Date: 2025.03.05 21:00:36 -06'00'

Firma del estudiante

Cédula: 1-1087-0929

Ilustración 79 - Carta Tutor

CARTA DEL TUTOR

Heredia, Costa Rica, 15 Marzo de 2025

MSc. Kattia Isabel Huertas Elizondo
Directora de la Escuela de Ingeniería Informática
Universidad Hispanoamericana

Estimada Sra.:

El estudiante **Roberto Valverde Quesada** , cédula de identidad número **110870929**, me ha presentado, para efectos de revisión y aprobación, el Proyecto de la **"DESARROLLO DE UNA PROPUESTA PARA LA IMPLEMENTACIÓN DE PROTOCOLOS BASADOS EN EL MARCO COBIT 2019 PARA LA GESTIÓN DEL DEPARTAMENTO DE TI DE LA EMPRESA SITEC S.A. (SISTEMAS INTEGRADOS DE SEGURIDAD S.A)",** el cual ha elaborado para optar por el grado académico de **Bachillerato en Ingeniería Informática.**

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por la postulante, se obtiene la siguiente calificación:

a)	ORIGINALIDAD DEL TEMA	10%	10%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20%
c)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	30%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	20%
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20%
	TOTAL	100%	**100%**

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Saludos,

RUBEN HEVER FALLAS PEÑA (FIRMA)

Digitally signed by RUBEN HEVER FALLAS PEÑA (FIRMA)
Date: 2025.03.15 13:15:14 -06'00'

Ing. Ruben H. Fallas Peña, MSc.

Ing. Rubén H. Fallas Peña, MSc. | Profesor Facultad de Ingeniería Informática Universidad Hispanoamericana | ruben.fallas@uh.ac.cr | Carné CPIC 6702 | Carné COLYPRO 60205

Ilustración 80 - Carta Lector

CARTA DE LECTOR

San José,

Universidad Hispanoamericana
Sede Llorente
Carrera de Informática

Estimado señor

El estudiante Roberto Valverde Quesada, cédula de identidad 1-1087-0929, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "Desarrollo De Una Propuesta Para La Implementación De Protocolos Basados En El Marco COBIT 2019 Para La Gestión Del Departamento De Ti De La Empresa Sitec S.A. (Sistemas Integrados De Seguridad S.A)".

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

Randall Vargas Villalobos

Firmado digitalmente por Randall Vargas Villalobos
Fecha: 2025.04.07 01:32:27 -06'00'

Firma
Randall Vargas Villalobos
Cédula: 1-1140-0113

Ilustración 81 - Carta CENIT

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 24 abril del 2025

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito Roberto Valverde Quesada con número de identificación 1-1087-0929 autor del trabajo de graduación titulado DESARROLLO DE UNA PROPUESTA PARA LA IMPLEMENTACIÓN DE PROTOCOLOS BASADOS EN EL MARCO COBIT 2019 PARA LA GESTIÓN DEL DEPARTAMENTO DE TI DE LA EMPRESA SITEC S.A. (SISTEMAS INTEGRADOS DE SEGURIDAD S.A) presentado y aprobado en el año 2025 como requisito para optar por el título de Bachillerato En Ingeniería Informática; (SI) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

ROBERTO VALVERDE QUESADA (FIRMA)

Digitally signed by ROBERTO VALVERDE QUESADA (FIRMA)
Date: 2025.04.24 09:05:44 -06'00'

_____
Firma y Documento de Identidad

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las "Condiciones de uso de estricto cumplimiento" de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

Ley De Certificados, Firmas Digitales Y Documentos Electrónicos Nº 8454 (SCIJ, 2025)
“Artículo 6º-Gestión Y Conservación De Documentos Electrónicos.

Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas.

La transición o migración a soporte electrónico, cuando se trate de registros, archivos o respaldos que por ley deban ser conservados, deberá contar, previamente, con la autorización de la autoridad competente.

En lo relativo al Estado y sus instituciones, se aplicará la Ley del Sistema Nacional de Archivos, Nº 7202, de 24 de octubre de 1990. La Dirección General del Archivo Nacional dictará las regulaciones necesarias para asegurar la gestión debida y conservación de los documentos, mensajes o archivos electrónicos.”

"Artículo 229 bis.- Daño informático (SCIJ, Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal, 2025)

Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable."

A continuación, se presenta una matriz de capacitación con información sobre empresas que ofrecen cursos gratuitos de ciberseguridad, incluyendo el nombre de la empresa, el curso, la duración, los costos y la referencia a Cisco, Palo Alto, Fortinet, MikroTik:

Tabla 12 - Matriz de capacitación

Nombre de la Empresa	Curso	Duración	Costo	Referencia
Fortinet	Programa de capacitación en ciberseguridad para profesionales de TI	Variable	Gratuito	Fortinet
Fortinet	Introducción al panorama de amenazas	Variable	Gratuito	Fortinet
Fortinet	Introducción a la ciberseguridad	Variable	Gratuito	Fortinet
Fortinet	Introducción técnica a la ciberseguridad	Variable	Gratuito	Fortinet
Palo Alto Networks	Cursos gratuitos de formación en ciberseguridad	Variable	Gratuito	Palo Alto
Cisco	Fundamentos Ciberseguridad	Variable	Gratuito	Netacad
Cisco	Administración de Amenazas Cibernéticas	Variable	Gratuito	Netacad
MikroTik	TCNA (Mikrotik Certified Network Associate)	Variable	Gratuito	Mikrotik Academy

Fuente: creación propia

Nota: La disponibilidad y los detalles de los cursos pueden variar. Se recomienda verificar la información actualizada en los enlaces proporcionados.

Formulario De Percepción

https://docs.google.com/forms/d/e/1FAIpQLSfhVy30YRTFFesI9JtvM0awLJie9rctb30Wlf8FH1Bgqq14eg/viewform?usp=dialog

ISO/IEC 27001:2022 Information Security, Cybersecurity And Privacy Protection — Information Security Management Systems — Requirements

https://www.iso.org/es/contents/data/standard/08/28/82875.html

ISO/IEC 27002:2022 Information Security, Cybersecurity And Privacy Protection — Information Security Controls

https://www.iso.org/es/contents/data/standard/07/56/75652.html

ISO/IEC 20000-1:2018 Information Technology — Service Management

https://www.iso.org/standard/70636.html

ISO 22301:2019 Security And Resilience — Business Continuity Management Systems — Requirements

https://www.iso.org/standard/75106.html

Cobit 2019

https://www.isaca.org/resources/cobit

Ley De Protección De La Persona Frente Al Tratamiento De Sus Datos Personales 8968

ARTÍCULO 5.- Principio de consentimiento informado

1.- Obligación de informar

Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco:

a) De la existencia de una base de datos de carácter personal.

b) De los fines que se persiguen con la recolección de estos datos.

c) De los destinatarios de la información, así como de quiénes podrán consultarla.

d) Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos.

e) Del tratamiento que se dará a los datos solicitados.

f) De las consecuencias de la negativa a suministrar los datos.

g) De la posibilidad de ejercer los derechos que le asisten.

h) De la identidad y dirección del responsable de la base de datos.

Cuando se utilicen cuestionarios u otros medios para la recolección de datos personales figurarán estas advertencias en forma claramente legible.

2.- Otorgamiento del consentimiento

Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.

No será necesario el consentimiento expreso cuando:

a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.

b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general.

c) Los datos deban ser entregados por disposición constitucional o legal.

Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos.

Glosario

Active Directory: Directorio activo de Microsoft para gestión de usuarios y equipos.

Adoption: Traducción al español “adoptar”.

Adversas: Contrario, enemigo, desfavorable.

Agile: Traducción al español “ágil”, metodología utilizada para mejorar los procesos.

Ámbito: Espacio comprendido dentro de límites determinados.

AP: Abreviatura de punto de acceso inalámbrico en inglés (Access Point).

APO: Administración por objetivos.

Azure: es la plataforma de computación en la nube creado por Microsoft para construir, probar, desplegar y administrar aplicaciones y servicios utilizando su infraestructura global.

Carece: Tener falta o privación de algo.

Cibercriminales: El cibercrimen es una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red, o bien que utiliza uno de estos elementos.

Ciberseguridad: La ciberseguridad es la tecnología, práctica y política para prevenir o mitigar los ataques cibernéticos.

Cobit: es un marco de trabajo para el gobierno y la gestión de las tecnologías de la información (TI) empresariales y dirigido a toda la empresa

Compilance: Se refiere al conjunto de prácticas y procedimientos implementados por una organización para asegurarse de que sus operaciones y actividades estén en conformidad con las leyes y regulaciones aplicables.

Dialéctico: es un método de argumentación y razonamiento que busca alcanzar la verdad a través de la confrontación y síntesis de ideas opuestas.

Directrices: es una norma o una instrucción que se tiene en cuenta para realizar una cosa.

Empíricos: es todo el saber que ha recopilado un individuo en su interacción con el mundo, sin recurrir al conocimiento científico.

Encriptar: En definitiva, consiste en cifrar: es decir, en transcribir un texto en signos (letras, números, etc.) de acuerdo con una determinada clave.

Endpoint: Traducción al español “Equipo final”, terminología utilizada para infraestructura.

ESU: (Extended Security Update) es un programa de pago que proporciona a las personas y organizaciones la opción de ampliar el uso de dispositivos Windows más allá de la fecha de finalización del soporte técnico de una manera más segura.

Fenomenología: Es una rama filosófica que estudia las manifestaciones del mundo desde la perspectiva de las personas.

Firewall: es un sistema de seguridad de red que restringe el tráfico de Internet entre las redes externas y internas.

Flyer: Medio impreso que se utiliza para transmitir información de manera concisa y visualmente atractiva.

Forum: Conocido como foro es un lugar físico o virtual donde se reúnen para intercambiar ideas y experiencias sobre diversos temas.

Goals: Es una palabra en inglés que se traduce al español como "objetivos". También puede traducirse como "metas".

IEC: La Comisión Electrotécnica Internacional (CEI), también conocida por su sigla en inglés IEC (International Electrotechnical Commission).

Implementation: La implementación es el acto de ejecutar un plan o proyecto, llevando a cabo las acciones necesarias para lograr los objetivos establecidos.

ISO: El significado de ISO es "Organización Internacional de Estandarización". Esta organización desarrolla y promueve normas que sirven como parámetros internacionales de calidad en productos, servicios y sistemas de producción.

Issues: traducido del inglés puede ser cuestión, tema, problema, asunto, edición, entre otros.

ITIL: Es el conjunto de buenas prácticas para gestionar y prestar servicios de TI de forma eficiente y de calidad.

Learning: Traducido al español como "aprendizaje". Se refiere al proceso de adquirir conocimientos o habilidades.

Malware: Es un término que se usa para referirse a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Management: Se refiere a la gestión o administración de una empresa u organización.

MFA: La autenticación multifactor, o MFA, es una forma de verificar la identidad del usuario que es más segura que la clásica combinación de nombre de usuario y contraseña.

Outsourcing: Se conoce como (neologismo del inglés: out, “fuera” y source, “fuente”), o como subcontratación, tercerización o externalización, al proceso empresarial

Polarización: es un proceso por el cual en un conjunto se establecen características que determinan la aparición en él de dos o más zonas, los polos, que se consideran opuestos respecto a una cierta propiedad, quedando el conjunto en un estado llamado estado polarizado.

Profile: Traducción del inglés “perfil”.

Ransomware: Es un tipo de malware que bloquea el dispositivo o cifra su contenido para extorsionar al propietario pidiéndole dinero. Su nombre proviene de la palabra inglesa "ransom", que significa "rescate"

Related: Traducción del inglés “relacionado”.

Requirements: Traducción del inglés “requerimientos”.

Resiliencia: En psicología se entiende como la capacidad que posee la persona para hacer frente a sus propios problemas, superar los obstáculos y no ceder a la presión, independientemente de la situación.

Risk: Traducción del inglés “riesgo”.

Role: Traducción del inglés “rol”.

Router: Traducción del inglés “enrutador”.

Service: Traducción del inglés “servicio”.

Size: Traducción del inglés “tamaño”.

Sourcing: Traducción del inglés “busqueda”.

Strategy: Traducción del inglés “estrategía”.

Tech: Traducción del inglés “tecnico”.

Threat: Traducción del inglés “amenaza”.

Vlan: Es un acrónimo que deriva de una expresión inglesa: virtual LAN. Esa expresión, por su parte, alude a una sigla ya que LAN significa Local Area Network. De este modo, podemos afirmar que la idea de VLAN refiere a una red de área local (lo que conocemos como LAN) de carácter virtual.

Wifi: Wi-Fi es el nombre comercial propiedad de la Wi-Fi Alliance para designar su familia de protocolos de comunicación inalámbrica

Bibliografía

ADEN.ORG. (11 de junio de 2024). *Metodologías ágiles: ¿Qué son y cuáles son las más utilizadas?* Obtenido de https://www.aden.org/business-magazine/metodologias-agiles/

ADVISERA.COM. (2022). *explanation of 11 new iso 27001 2022 controls*. Obtenido de https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/

Araujo, H. A. (s.f.). *ISO 27001: ¿Cómo crear el plan de concientización y capacitación de tu empresa?* Obtenido de https://blog.hackmetrix.com/plan-de-concientizacion-y-capacitacion-seguridad/

Capitalis. (24 de julio de 2019). *La importancia de una Política de Seguridad de la Información*. Obtenido de https://capitalis-it.com/la-importancia-de-una-politica-de-seguridad-de-la-informacion/

CEC. (09 de 11 de 2020). Obtenido de https://www.cec.es/buenas-practicas-para-mejorar-la-seguridad-de-tu-oficina-en-casa/

CEPYME. (17 de 09 de 2024). *Qué es una política de contraseñas y cómo crear una*. Obtenido de https://cepymenews.es/politica-contrasenas/

CONCEPTO.DE. (2024). *¿Qué es el marco metodológico?* Obtenido de https://concepto.de/marco-metodologico/

Consulting, J. I. (2025). *Služby informační bezpečnosti ICT – Trendy 2025*. Obtenido de https://jecom.cz/bezpecnost-ict/

CYBERSECURITY360. (27 de 12 de 2022). *Aikido Wiper manipola gli antivirus per cancellare file anche senza permessi privilegiati: come difendersi*. Obtenido de https://www.cybersecurity360.it/nuove-minacce/aikido-wiper-manipola-gli-antivirus-per-cancellare-file-anche-senza-permessi-privilegiati-come-difendersi/

DELTAPROTECT. (21 de 05 de 2024). *Seguridad de la red: ¿Qué es, cómo funciona y qué tipos existen?* Obtenido de https://www.deltaprotect.com/blog/seguridad-de-la-red

Excelencia, E. E. (27 de agosto de 2019). *Clasificación de la información según ISO 27001*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2019/08/clasificacion-de-la-informacion-segun-iso-27001/

explicados, 7. t. (08 de 02 de 2024). *TECNO*. Obtenido de https://tecno-simple.com/7-tipos-de-copias-de-seguridad-de-datos-completamente-explicados/

FANDOM. (s.f.). *Las terminales*. Obtenido de https://ticstrabajoescolar.fandom.com/es/wiki/Las_terminales

Group, E. (10 de 12 de 2015). *Eliminación segura de documentos según la norma ISO 27001*. Obtenido de https://www.pmg-ssi.com/2015/12/eliminacion-segura-documentos-segun-norma-iso-27001/

HACKHISPANO:COM. (2012). *Norma ISO 27032: Gestión de la Ciberseguridad*. Obtenido de https://foro.hackhispano.com/threads/45794-Norma-ISO-27032-Gesti%C3%B3n-de-la-Ciberseguridad

HOBBS.UK. (2022). *We have recently secured ISO 22301 for Effective Business Continuity*. Obtenido de https://hobbs.uk.com/insights/iso-22301/

IBM.COM. (s.f.). *¿Qué es una ITIL?* Obtenido de https://www.ibm.com/mx-es/topics/it-infrastructure-library

INVENSISLEARNING.COM. (2019). *COBIT 2019 DESIGN FACTORS*. Obtenido de https://www.invensislearning.com/blog/cobit-2019/

ISACACR.ORG. (2024). *COBIT 2019*. Obtenido de https://www.isacacr.org/certificaciones.html#undefined5

ISMS.ONLINE. (2022). *ISO 27002:2022, Security Controls. Complete Overview - ISMS.online*. Obtenido de https://www.isms.online/iso-27002/

ISO, N. (s.f.). *Seguridad de la Información y control de accesos*. Obtenido de https://www.normas-iso.com/seguridad-de-la-informacion-y-control-de-accesos/

ISO.ORG. (2022). *¿Qué es ISO/IEC 27002?* Obtenido de https://www.iso.org/es/contents/data/standard/07/56/75652.html

ISOTools.ORG. (2022). *¿Qué es la ISO 27001?* Obtenido de https://isotools.org/isotools/normas/sistema-de-gestion-de-riesgos-y-seguridad/iso-27001/

ISOTools.US. (2016). *ISO 20000: ¿Por qué es buena idea implementarla en tu organizacion?* Obtenido de Una metodología con enfoque para gestionar los servicios TI y así demostrar que la organización hace uso de mejores prácticas

ISOTools.US. (2024). *Sistema de Gestión de Continuidad de Negocio*. Obtenido de https://www.isotools.us/normas/riesgos-y-seguridad/iso-22301/

Jessyca. (9 de 10 de 2021). *¿Cómo crear una contraseña segura?* Obtenido de https://adamcod.es/contrasena-segura/

Microsoft. (18 de 05 de 2023). *Finaliza el soporte para Windows Server 2012 y 2012 R2*. Obtenido de https://learn.microsoft.com/es-es/lifecycle/announcements/windows-server-2012-r2-end-of-support

Microsoft. (s.f.). *Acceso a cuentas de usuario en Windows*. Obtenido de https://support.microsoft.com/es-es/windows/acceso-a-cuentas-de-usuario-en-windows-8f1f3c05-e479-4e9a-666b-90091d052aaf

Neskey, C. (2024). *Cuánto tiempo le toma a un hacker robar tu contraseña*. Obtenido de https://www.hivesystems.com/blog/are-your-passwords-in-the-green

NORMASISO.ORG. (s.f.). *¿Qué es la norma ISO 27032?* Obtenido de https://normasiso.org/norma-iso-27032/

OCDTECH. (s.f.). *GESTION DE ACCESO PRIVILEGIADO: PAM*. Obtenido de https://ocd-tech.com.mx/2023/05/accesoprivilegiadopam/

Picheta, R. (22 de abril de 2019). *Estas son las contraseñas más "hackeables" de internet*. Obtenido de https://cnnespanol.cnn.com/2019/04/22/estas-son-las-contrasenas-mas-hackeables-de-internet/

proactivanet.com. (s.f.). *Axelos completa la publicación de las 34 prácticas de ITIL 4*. Obtenido de https://www.vrogue.co/post/axelos-completa-la-publicaci%C3%B3n-de-las-34-pr%C3%A1cticas-de-itil-4

pxhere. (s.f.). Obtenido de https://pxhere.com/en/photo/641575

Sampieri, D. R. (2014). *Metodología de la investigación.* México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Sánchez, O. (2014). *Mejores prácticas de TI: Más valor para el negocio*. Obtenido de https://www.computerweekly.com/es/cronica/Mejores-practicas-de-TI-Mas-valor-para-el-negocio

SEAM. (23 de marzo de 2023). *3 Principles of Personal Information Retention and Disposal*. Obtenido de https://seamservices.com/blog/3-principles-of-personal-information-retention-and-disposal/

SitecSeguridad. (2010). *www.sitecseguridad.com*. Obtenido de www.sitecseguridad.com/nosotros/

STUDIO, K. (s.f.). *Ilustración exclusiva derechos de acceso concepto de tendencia*. Obtenido de https://www.freepik.es/vector-premium/ilustracion-exclusiva-derechos-acceso-concepto-tendencia-ilustracion-plana_90980301.htm

Team, N. G. (18 de 01 de 2024). *DoD 5220.22-M vs NIST 800-88 — ¿Cuál es mejor para su negocio?* Obtenido de https://nsysgroup.com/es/blog/dod-5220-22-m-vs-nist-800-88-which-is-better-for-your-business/

TECNOGEEK. (s.f.). *Autenticación de dos factores: Cómo esta medida de seguridad puede ayudarle a protegerte online*. Obtenido de https://tecnogeek.net/autenticacion-de-dos-factores-como-esta-medida-de-seguridad-puede-ayudarle-a-protegerte-online/

WebMaster. (3 de agosto de 2023). *La importancia de los acuerdos de no divulgación (NDA) en la protección de la información confidencial*. Obtenido de

https://www.alvamark.com/blog/la-importancia-de-los-acuerdos-de-no-divulgacion-nda-en-la-proteccion-de-la-informacion-confidencial/

YASM.COM. (2024). *Why ISO 20000? 5 main benefits*. Obtenido de https://yasm.com/wiki/en/index.php/ISO_20000

Fortinet

Palo Alto Networks

Cisco

Cisco Networking Academy

MikroTik Academy

Trabajo de Auditoria: Normas COBIT

Sistema de gestión de denuncias: elemento clave para la gobernanza de las organizaciones

La norma 27001 y su importancia en seguridad de la información IT