# Planificación del sistema de gestión de seguridad de la información (SGSI) de la empresa International Protection.

Jorge Luis Dau Janne

Darinel Senon Contreras Pérez

Universidad Nacional Abierta Y A Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería

Ingeniería De Sistemas

Barranquilla

2022

# Planificación del sistema de gestión de seguridad de la información (SGSI) de la empresa International Protection.

Jorge Luis Dau Janne

Darinel Senon Contreras Pérez

Proyecto De Grado

Obtener El Título De Ingeniero De Sistemas

Asesor

Mario Ávila Pérez

Universidad Nacional Abierta Y A Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería

Ingeniería De Sistemas

Barranquilla

2022

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Barranquilla, 2022

## Dedicatoria

A Dios, quien da el conocimiento, la inteligencia y la sabiduría en toda ciencia

Y a nuestras familias que han tenido fe y sacrificio por nuestros sueños

**Agradecimientos**

Deseamos agradecer a todos aquellos que desde la referencia técnica y acompañamiento generaron valor significativo en la capacidad de poder concluir este proyecto, y especialmente a nuestro asesor Mario Ávila, quien hizo posible su materialización.

**Resumen**

A partir del Modelo de la Seguridad y Privacidad de la Información (MSPI), publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia y que imparte lineamientos en materia de implementación y adopción de buenas prácticas con referencia en estándares internacionales, el presente proyecto desarrolla las fases de diagnóstico y planificación del Sistema de gestión de seguridad de la información (SGSI) en la empresa International Protection.

El Modelo de la Seguridad y Privacidad de la Información (MSPI), inicialmente diseñado y publicado para las entidades públicas y que también permite el alcance a terceros que deseen implementar el modelo, orienta la gestión e implementación adecuada del ciclo de vida de la seguridad de la información a través de 5 fases (Diagnóstico, Planeación, Implementación, Evaluación, Mejora Continua).

El presente proyecto abarca las fases de diagnóstico y de planeación, de acuerdo con los modelos metodológicos propuestos. Inicialmente se realiza el diagnóstico con el reconocimiento actual de la empresa, identificación del nivel de madurez y levantamiento de la información, previo a la fase de planificación que cuenta con 4 momentos (contexto, liderazgo, planeación y soporte) con la mira de acordar acciones para la seguridad y privacidad de la información.

Palabras clave: normas, modelo, vulnerabilidades, planificación, lineamientos, integridad, disponibilidad, seguridad.

## Abstract

Based on the Information Security and Privacy Model (MSPI), published by the Ministries of Information and Communications Technologies in Colombia and which provides guidelines on the implementation and adoption of good practices with reference to international standards, this project develops the diagnostic and planning phases of the Information Security Management System (SGSI) in the company International Protection.

The Information Security and Privacy Model (MSPI), initially designed and published for public entities and which also allows the reach to third parties who wish to implement the model, guides the management and proper implementation of the information security lifecycle through 5 phases (Diagnosis, Planning, Implementation, Evaluation, Continuous Improvement).

This project covers the diagnostic and planning phases, according to the proposed methodological models. Initially, the diagnosis is carried out with the current recognition of the company, identification of the level of maturity and collection of information, prior to the planning phase that has 4 moments (context, leadership, planning and support) with the purpose of defining the actions to be implemented at the level of security and privacy of the information.


Keywords: standards, model, vulnerabilities, planning, guidelines, integrity, availability, security.

# Tabla de Contenido

## Lista de tablas

## Lista de figuras

## Introducción

En el mundo de la hiperconectividad, de la rapidez y de la omnipresencia, la información, como medio para alcanzar el bienestar de necesidades de las personas y los negocios, pasó a ser un recurso con sus propios desafíos, que amerita un tratamiento cuidadoso y seguro. Hoy la información es mucha, y la forma como se almacena, se usa y cómo se comparte, ha tenido transformaciones grandemente valiosas para el desarrollo del ser humano y la sociedad; sin embargo, al ser un recurso, este debe ser adecuadamente tratado y reconocido como elemento de los objetivos estratégicos de las compañías y como medio para la complacencia de las necesidades del humano.

La sostenibilidad, reconocida como la acción de permanecer en el tiempo haciendo buen uso de los recursos presentes, garantizando su existencia al futuro (inclusive para generaciones venideras) y permitiendo la satisfacción de todas las partes interesadas, invita a tener una visión más global y proyectiva de los negocios, con la identificación y gestión de los procesos estratégicos, operativos y de soporte. Es decir, que, para el avance de la actividad financiera de una organización, se debe tener una mirada abierta e integral.

La información, en cuanto a la confidencialidad, integridad y disponibilidad, deben hacer parte de los objetivos estratégicos de la compañía desde el inicio; presente en el establecimiento de los objetivos del negocio, la planeación, el modelo estratégico y una filosofía compartida por todas las partes interesadas. Al realizar un análisis de contexto en la empresa INTERNATIONAL PROTECTION, se evidencia que realiza tratamiento de información importante para la operación y que esta no tiene un modelo metodológico definido que procuren la seguridad y privacidad.

El presente proyecto, es una propuesta de inicio a un modelo para la seguridad y privacidad de la información en la empresa International Protection, tomando como referencia el modelo publicado por el Ministerio de Tecnologías de la información y las comunicaciones en Colombia (MSPI-MinTics), que, si bien la inspiración inicial del MSPI son las empresas públicas del país, permite ser extensivo a terceros del sector privado. Este mismo modelo de Mintics, toma como referencia la NTC-ISO/IEC 27001 (ICONTEC, 2006) y se define en 5 etapas (Contexto, planificación, operación, evaluación de desempeño y mejoramiento continuo).

El presente proyecto, fue desarrollado en las 2 primeras etapas (contexto y planificación), y pretende contribuir al inicio de un modelo de seguridad y privacidad de la información, que sea considerado dentro de los procesos estratégicos de la compañía y que sea inspiración para el reconocimiento del recurso de la información con debilidades, oportunidades, fortalezas y amenazas. Finalmente, y de acuerdo con su desarrollo en la etapa de contexto y planificación, se define las acciones para abordar los riesgos, así como los planes y objetivos de cada una de ellas.

## Planteamiento del problema

La información en las empresas es unos de los recursos esenciales, importantes, cotidianos y vulnerables, que se ve en constante relación con actores internos y externos en la compañía; además, de todas las afectaciones a las que se ve expuesta en el dinamismo diario de su misma naturaleza. La efectiva administración que permita la disponibilidad, integridad y seguridad de los datos, contribuye de forma directa a la sostenibilidad de la empresa.

En la actualidad parece incuestionable que el triunfo de la organización no dependería exclusivamente de cómo utilice sus activos materiales, sino también de la tarea de gestionar los recursos de la información. Algunos escritores suponen que las empresas deben ser estimadas como sistemas de información. (Morales, 2004).

La solución planteada para este problema es iniciar un modelo metodológico de Seguridad y Privacidad de la información, con la planificación del SGSI, bajo modelos nacionales (Modelo de seguridad y privacidad de la información, MINTIC) y estándares internacionales (NTC-ISO/IEC 27001). Este proyecto contribuye a que las partes de interés tomen decisiones asertivas respecto a la seguridad (disponibilidad, integridad y confidencialidad) en las operaciones diarias (Santos Llanos, D. E. 2016).

La empresa INTERNATIONAL PROTECTION cuenta con 30 empleados, cada uno con computador asignado y con una red de datos estructurada, inalámbrica y cableada. En la actualidad, se han presentado perdida de datos, manejo de información confidencial y vulnerable por usuarios no autorizados, no existe un procedimiento para el acceso a la información; inconvenientes en la seguridad, que comprometen la disponibilidad, integridad y confidencialidad de la información en la empresa.

**Formulación del problema**

¿Cómo la planificación del modelo de seguridad y privacidad de la información (MSPI) ayudará a minimizar las vulnerabilidades y amenazas de seguridad de la información que se presentan en la empresa INTERNATIONAL PROTECTION de la ciudad de Barranquilla?

# Objetivos

## Objetivo general

Planificar el sistema de gestión de la seguridad de la información de la empresa International Protection, para garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación del modelo MINTIC (MSPI).

## Objetivos específicos

Identificar el estado actual de la gestión de seguridad y privacidad de la información en la empresa International Protection, mediante el diagnóstico del estado actual.

Realizar la planificación del sistema de seguridad de la empresa que satisfaga las necesidades de seguridad y privacidad de la información, aplicando las recomendaciones de las guías del MSPI.

Determinar los riesgos y definir las acciones para valorarlos precisando el plan de tratamiento sobre ellos.

## Justificación

En la actualidad, International Protection, presenta incidentes de seguridad en cuanto a la información, que reflejan vulnerabilidades en cuanto a disponibilidad, integridad y seguridad de la información y que podría llegar a representar una real amenaza para la sostenibilidad del negocio; reconociendo que diariamente se hace uso, consulta, administración y almacenamiento de datos, en las acciones naturales de la empresa.  Es decir, que la información es un recurso valioso para el negocio.

Por lo tanto, se reconoce la necesidad de iniciar el diseño de un sistema de gestión de la seguridad de la información SGSI, que intervenga las brechas actuales, que se anticipe y también que genere los procesos para disminuir el impacto no deseado, referente a la seguridad de la información. El modelo para la seguridad y la privacidad de la información elaborado y publicado por MINTIC, contribuye a la intervención del problema identificado, ofreciendo lineamientos, metodologías e instrumentos para obtener los objetivos planteados en el presente proyecto.

Si bien el modelo propuesto contempla 5 fases (diagnóstico, planear, hacer, verificar y actuar), el proponer el inicio del SGSI con la fases de diagnóstico y planificación, aportará a reconocer el problema, reconocer el contexto y la realidad actual de la empresa y el negocio, las expectativas, a promover el compromiso de las partes concernidas en la gestión del recurso del dato, a disponer de acciones, recursos y responsables para la gestión de la seguridad y la privacidad y definir procedimientos para la seguridad de la información, que en ultimas tendrá un impacto directo e indirecto en la sostenibilidad y permanencia de la empresa en el mercado.

En primer lugar, este proyecto tiene como finalidad que la empresa International Protection, cuente con un sistema de seguridad y privacidad de la información bastante robusto y seguro, que les permita realizar una detección temprana de vulnerabilidades y amenazas a su sistema informático, y que cuente con procesos y procedimientos que les garantice la disponibilidad, integridad y confidencialidad de la información de la empresa.

El desarrollo de este proyecto es pertinente para la UNAD, ya que aporta a los estudiantes los conocimientos necesarios para poder presentar sus proyectos aplicados para graduarse, de las carreras que pertenecen a la Escuela de Ciencias Básicas Tecnología e Ingeniería, involucrando un importante tema como lo es la planificación de un sistema de seguridad y privacidad de la información en las empresas u organizaciones públicas y privadas. La pertinencia se sustenta en la consecución de los elementos y aspectos importantes para la generación de nuevas iniciativas para la planificación y el mejoramiento continuo de los procesos de seguridad de la información en las empresas u organizaciones.

En este mismo sentido, este proyecto tiene pertinencia en el ámbito social toda vez que a través de los resultados se benefician también las grandes y pequeñas empresas en la medida en la que mejoren los procesos que permitan y garanticen la seguridad de la información.

Finalmente, este proyecto es viable desde el panorama de recurso humano, ya que éste se justifica con base a los conocimientos alcanzados en este proyecto aplicado ya que ofrecen a los autores de este proyecto de las destrezas y conocimientos que requiere la planeación, documentación y ejecución de este.

# Marco de referencia

## Antecedentes

En el año 2017 se divulgó el trabajo titulado “Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa GEOSURVEY de la ciudad de lima, Perú”. El cual expone un sistema de gestión de la seguridad de la información bajo el ISO 27002 para optimizar la seguridad en todo lo que haga referencia al uso de los activos y tecnologías de la información en la organización. Las técnicas a utilizar fueron bajo el enfoque cuantitativo, y de tipo aplicativo; porque se utilizó la tecnología para la solución de un problema.

La población y la muestra estuvieron conformadas por 33 colaboradores estando no probabilística, cubriendo todas las áreas de la empresa. A través del cuestionario se recolecto los datos, por lo que el instrumento de fuente de información fue el cuestionario y los datos hallados fueron procesados por el software estadístico SPSS. Los resultados permitieron inspeccionar y optimizar la seguridad de la información de la compañía, mediante un dictamen de la gestión de riesgos. (Vilca Mosquera, E. C. 2017)

Por otra parte, se tiene el proyecto divulgado en el año 2016 titulado “Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001:2013 para la red corporativa de la empresa ecuatoriana ECUATRONIX”. Para dar inicio al proyecto se hizo necesario tener claridad de los nuevos objetivos de control, consolidados en la actualización de la norma ISO/IEC 27001:2013, se realizó el reconocimiento del centro de datos para los activos, reconocer sus amenazas y riesgos, definir los criterios de mitigación del riesgo. La

arquitectura de procesos denominada PDCA define un espectro de amenazas, agrupadas en tres grupos: humanas, tecnológicas y naturales, y sobre esta arquitectura se desarrolló el SGSI. (Villacís Espinosa, M. L. 2016)

En este mismo sentido en el contorno nacional, se halla el trabajo de investigación titulado "Diseñar un Sistema de Gestión de la Seguridad de la Información para la Empresa Qwerty S.A a partir de la Norma ISO 27001". Donde a partir de todo un documento estructurado se presenta el inicio del diseño de un sistema de gestión de la seguridad de la información para la compañía QWERTY S.A, estimulada en la norma ISO 27001:2013. Plantea la iniciación del diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI), mediante un grupo de ciclos agrupadas, que inicia con el estudio de los activos de la compañía, identificación de los riesgos y amenazas en el área de Infraestructura, analiza la gestión de riesgos con la metodología conocida como Margerit y da fin a la propuesta de las políticas en cuanto a seguridad se refiere. (Gómez Ravelo, C. A. 2020)

También se cuenta con la investigación titulada "Propuesta de un plan estratégico de seguridad y privacidad de la información para el Departamento Administrativo de la Función Pública (DAFP)". El objetivo principal es aportar a la seguridad y privacidad de la información en la institución pública, mediante el Modelo MSPI de la Mintic. En el análisis de la propuesta, se reconoció que la DAFP no tiene identificados los riesgos y vulnerabilidades, así como las áreas expuestas. Como aspectos adicionales, se investigó en la fortaleza de éxito de la seguridad y privacidad de la información en otras empresas, lo que proporciono elementos para el diseño de criterios para asegurar la privacidad de la información, el diseño de procesos y fortalecer las

capacidades de los individuos involucrados en la seguridad de la información. (Olmos Sosa, O y Quesada Pérez, I. 2019)

Los diferentes autores coinciden que estamos en la época de la información y se despliegan datos numerosos en las organizaciones, convirtiéndose en activos importantes. En un evento natural, donde la empresa sufriera una perdida física, esta podría ser corregida; en cambio, si se llegara comprometer la información y la empresa no cuenta con las consideraciones debidas, sería muy difícil su recuperación, generando impactos en la vida y estabilidad de la empresa. (Aguirre Cardona & Aristizábal Betancourt, 2013)

**Marco teórico**

En el análisis de tendencias de consumo y las formas como hoy se satisfacen las necesidades, se ha identificado la hiperconectividad y la facilidad de conexiones, como un fenómeno de grande e ininterrumpido crecimiento, llevando a que la información constantemente este en aumento, movimiento y transformación. En la actualidad, una gran parte de las organizaciones cuentan con una red de conexión y los datos viajan permanentemente a diferentes lugares del mundo. Es sin duda una gran fortaleza, pero también un reto que requiere control de la información; recientemente ha dejado pérdidas significativas que afectan la estabilidad, economía y reputación empresarial, y al parecer cada día hay mayores amenazas. (Menéndez et al., 2009)

En las organizaciones la seguridad de la información era consideraba solamente como gasto general, ahora se ha transformado en inversión para las empresas; y se enfrenta, constantemente, a retos de justificación económicas de inversiones importantes que deben ser

argumentados por los equipos responsables, respondiendo preguntas de cómo, por qué, para que, con quien. (Cárdenas-Solano, L. J., Martínez-Ardila, H., & Becerra-Ardila, L. E. 2016)

Para dar respuesta a estas tendencias y búsqueda de satisfacer necesidades, la tecnología ha sido adaptativa, amigable y accesible; sin embargo, al mismo tiempo las vulnerabilidades en seguridad y privacidad de la información aumentan, a nivel individual como organizacional. Es por eso la necesidad de implementar medidas de seguridad que protejan el activo del dato en las organizaciones. (Vega Velasco, W. 2008)

González (2011), reseña a la seguridad de la Información como la disciplina, que percibe las amenazas, las vulnerabilidades, los estudios de escenas, las buenas prácticas y esquemas normativos, involucrando el aseguramiento de métodos y tecnologías para privacidad, disponibilidad y aseguramiento de la información.

Rojas Valduciel (2016), describe la protección de los datos como las medidas y actividades que protegen los activos de información, mitigando y manteniendo la inseguridad a unos niveles admisible.

La seguridad de la información es entendida como la conservación de las confidencialidades, integridades y disponibilidades de la información (NTC-ISO/IEC 17799:2006). Para este proyecto se tomó como principales referencias de acciones que permitan garantizar la seguridad 2 documentos técnicos (NTC ISO/IEC 17001:2006 y Modelo MSPI de la MINTIC), aun cuando varios autores afirman que no es posible llegar a un 100% de efectividad, por la naturaleza misma del dato en tiempos actuales y venideros.

La confidencialidad de la información hace referencias a que la propiedad detalla que el dato no sea disponible ni revelado (NTC 5411-1:2006). Esta información es considerada valiosa

para la compañía y hace parte del funcionamiento del negocio, que, en manos equivocadas o no autorizadas, podría traer consecuencias dañinas. La compañía debe reconocer qué información debe y puede ser de dominio para los usuarios, cómo implementar protocolos de seguridad para mantenerla y cuáles son las acciones de contingencia.

Por otro lado, la integridad se refiere a que la propiedad garantiza el estado original e integral de su estado (NTC 5411-1:2006), acción declaratoria de que los datos son un recurso valioso y se asignan los recursos necesarios para tal fin. Y, por último, sin ser el menos importante, la disponibilidad, que la que conlleva a que la información pueda ser accesible y también utilizada cuando así lo requiera el usuario (NTC 5411-1:2006), en el momento que lo requiera, respondiendo a cumplimientos internos y externos.

La (Norma técnica colombiana – ISO 27001) adaptada establecidas por las normas ICONTEC en el 2006, a partir de la norma ISO/IEC 27001, ofrece un modelo para establecer, implementar, operar, seguir, revisar, mantener y mejora un sistema de gestión de la seguridad de la información (SGSI). Permitiendo su adaptación a las diferentes particularidades que puede tener cada organización; tal cual como lo menciona la norma: una situación simple requiere una solución de SGSI simple. (ICONTEC, 2006)

Sin embargo, cuando una empresa realiza la declaración de conformidad a la norma, esta debe ser implementada con todos sus requisitos, conforme lo establece, salvo cuando la exclusión de controles del requisito no afecte la capacidad y la seguridad y esta pueda ser evidenciada. Una empresa que cuente con la implementación de NTC-ISO 9001:2000 y la NTC-ISO 14001:2004, podría integrar el SGSI, ya que está diseñada con esta posibilidad y la satisfacción de los requisitos se dan de forma integrada.

Por otro lado, la MINTIC en Colombia, elaboró y publico el Modelo de seguridad y privacidad de la información (MSPI), que considera las buenas prácticas para la gestión de la información para las organizaciones públicas. Este modelo, permite ser usado por terceros (inclusive entidades privadas) que consideran valioso el uso de esta metodología para la seguridad y privacidad de la información de su empresa. El modelo cuenta con un conjunto de documentos asociados para optimizar los modelos de seguridad de los datos y con guías para cada fase. El modelo metodológico, está basado en 5 fases: diagnóstico, planear, hacer, verificar y actuar.

A nivel internacional la Organización (OECD), que tiene como misión el crear excelentes estrategias para una existencia sobresaliente y a la que Colombia recientemente se unió (28 de abril de 2020), publicó por primera vez, en 1992, las directrices de Seguridad y el 25 de julio de 2002, las directrices para la seguridad de los sistemas y redes de datos: hacia un saber de seguridad. (Organization for Economic Co-operation and Development (OECD) y Ministerio de Administraciones Públicas, Secretaría General Técnica, 2004)

La gestión de la seguridad de la información desafía una alta responsabilidad de la organización, agudeza técnica y metodológica para la identificación, intervención del riesgo, seguimiento de las acciones y constancia para renovar y actualizar conforme al dinámico ambiente que rodea las organizaciones sostenibles.

## Marco conceptual

### *Análisis de riesgos*

Es el proceso que admite evaluar los riesgos. Para el análisis, lo principal que se debe hacer es la identificación de los activos con los que cuenta la compañía. La evaluación de riesgos

establece una comparación de entre la nivelación del peligro identificado con los criterios de riesgo establecidos preliminarmente. La función es lograr una nivelación prudente de aprobación a los objetivos en mención y certificar como mínimo el despliegue del indicador estratégico con los que se realiza la evaluación, el monitoreo y la mejora. (Nieves, A. C. 2017)

Los resultados alcanzados del análisis van a aprobar la utilización de cierto método para el tratamiento del riesgo, evaluarlos, tomar medidas para planear el procedimiento y ejecución.

El estudio de los riesgos facilita la generación de un enfoque riguroso en la identificación de los factores de riesgo presentes en la empresa. La identificación de vulnerabilidades y amenazas permite minimizar con acciones operativas la perdida de datos. (Heredero, y otros, 2006)

***Seguridad informática***

"Es la protección frente a todos los daños sufridos o producidos por la herramienta informática y producidos por el evento voluntario y de mala fe de un sujeto". Para optar una seguridad apropiada, se deben de implementar acciones que establezcan restricciones para los usuarios, los recursos financieros facilitadores de las medidas, el tiempo para el desarrollo de las acciones y el mantenimiento y mejoras en las instalaciones. (Royer, 2004)

***Confidencialidad***

Son las particularidades que afirman que las personas, procesos, etc., no tengan manipulación de los datos a menos que tengan autorización. (Cerra, 2010)

***Disponibilidad***

Es garantizar que los recursos de los sistemas y los datos estén disponibles solo para usuarios con autorización en el instante que lo necesiten. (Cerra, 2010)

***Integridad***

Dice que la alteración de los datos solo sea ejecutada por usuarios con autorización, por intermedio de los diferentes procesos con autorización. (Cerra, 2010)

***Sistema de gestión de seguridad***

Son medidas que engloba una serie de acciones para valorar las amenazas y saber su estado. Se basa en los riesgos de la empresa y en el saber que se establece y promueve la mejora en la protección de los datos. Esta contiene una responsabilidad de la empresa y detalle de las actividades para las buenas prácticas para salvaguardar los datos. (Bertolín, 2008)

***Norma técnica ISO/IEC 27001***

ISO 27001 es una norma internacional presentada por la Organización Internacional de Normalización (ISO) y puntualiza cómo realizar la gestión referente a la seguridad de los datos en una organización. La investigación más nueva fue divulgada en el 2013 y hoy llamada ISO/IEC 27001:2013. En el año del 2005 fue publicada la revisión inicial y se realizó basado en la normalización británica BS 7799-2.

La idea central de la ISO 27001 es salvaguardar las confidencialidades, integridades y disponibilidades de la información en una organización, mediante el reconocimiento de riesgos que afectarían la información y con la definición de acciones y recursos necesarios para evitar, mitiga o el riesgo.

Por lo cual, lo principal de la norma ISO 27001 es basarse en la gestión de riesgos: indagar los riesgos y luego tratarlos de una manera sistemática. (Academic, 2015)

***Modelo de la seguridad y la privacidad de la información – MSPI***.

Son los lineamientos para la ejecución de buenas prácticas en la seguridad de la información. El modelo es diseñado para las entidades públicas en Colombia, sin embargo, el documento extiende sus beneficios a terceros del sector privado. Toma como base metodológica y legal estándares internaciones, como ISO/IEC 27001 y otros nacionales.

**Marco legal**

- La ley 527 de 1999 - “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras”. (República de Colombia, ley 527, 1999)
- La ley 1266 de 2008 - “por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en las bases de datos personales, en especial la financiera, crediticia, comercial, deservicios y la proveniente de terceros países y se dictan otras disposiciones". (República de Colombia, ley estatutaria 1266, 2008)
- La ley 1273 de 2009 - “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. (República de Colombia, ley 1273, 2009)

- La ley estatutaria 1581 de 2012 - “Por la cual se dictan disposiciones generales para la protección de datos personales.” (República de Colombia, ley estatutaria 1581, 2012)
- La ley 1582 de 2012 - “por la cual se dictan disposiciones generales para la protección de datos personales”. (Congreso de la república ley 1582, 2012)
- Decreto 2106 de 2019, implanta que las autoridades que efectúen trámites, procesos y procedimientos por medios digitales, deben tener la disposición de una táctica de seguridad digital de acuerdo a los lineamientos de la autoridad competente.

# Metodología

## Tipo de investigación

Para este estudio se adoptó el diseño de investigación descriptivo teniendo en cuenta que se utilizan datos específicos para la planificación de un modelo de la seguridad y privacidad de la información MSPI, concebidos a partir de la información recolectada de los empleados de la empresa.

La propuesta de investigación considera el empleo de una aproximación cuantitativa, con una estrategia basada en encuesta, usando el método de cuestionarios.

El cuestionario estará dirigido a los empleados de la empresa o de todos aquellos que participen en la implantación del modelo de la seguridad y privacidad de la información MSPI de la MinTic.  para la gestión de la seguridad de la información en la empresa, usando como herramienta cuestionarios creados para tal fin. El trabajo de campo estará apoyado en la realización de la encuesta y comprende el diseño, desarrollo, validación, distribución de la encuesta, y la recolección de la información obtenida para su correspondiente análisis.

## Enfoque

La actual investigación se asienta en el enfoque cuantitativo y el diseño de esta es descriptivo con el propósito de la creación de un modelo de la seguridad y privacidad de la información en la empresa International Protection. El enfoque cuantitativo se hace palpable ya que algunos datos son mostrados cuantitativamente, no obstante, se hace la representación o el significado de esos datos. Este proyecto busca la planificación de un sistema de seguridad y privacidad de la información, que permita la minimización de los riesgos en cuanto amenazas y

vulnerabilidades de la información, a partir de la información recolectada de los empleados de la empresa International Protection.

Para la gestión de la confidencialidad, integridad y disponibilidad de los sistemas de la información, se dio inicio con las 2 primeras fases, diagnóstico y planificación, del Modelo de Seguridad y Privacidad de la Información de MINTIC (MSPI, MINTIC 2021)

**Figura 1**

*Ciclo del MSPI (MINTICS, 2021)*


*Nota.* En esta figura se muestra el Ciclo del MSPI (MINTICS, 2021)

A continuación, se definen las fases y actividades sumidas en el marco metodológico: La fase 1 de diagnóstico.

- Realizar un análisis GAP (análisis de brechas de necesidades, a partir del estado actual y el estado objetivo)
- Realizar encuesta de diagnóstico.

Fase 2 de planificación.

- Conocer la estructura organizacional vertical, con responsables de procesos y personas de forma directa.
- Realizar una tabla donde se describa la necesidad y expectativa de las partes interesadas en la empresa International Protection bajo el modelo MSPI.
- Conocer las políticas que se les aplica a los trabajadores, terceros, aprendices, practicantes y proveedores, referente a la seguridad de la información.
- Realizar tabla para describir autoridad, funciones y responsabilidades de las partes interesadas en International Protection, dentro del MSPI.
- Utilizar la Guía N°5 para la Gestión y Clasificación de Activos de Información (Modelo de seguridad y privacidad de la información, MINTICS).
- Realizar la Identificación de amenazas de los activos, de acuerdo al modelo propuesto en la guía N°7, del Modelo de Seguridad y privacidad de la información del Mintics
- Desarrollar tabla con los Ítems del plan de tratamiento de riesgos (ISO 27002 - Controles de seguridad)

# Desarrollo

## Identificación del estado actual de la gestión de seguridad y privacidad de la información.

### *Fase 1. Diagnóstico*

Esta etapa, se identificó el estado actual, pero también los niveles de expectativa de la gestión de seguridad y privacidad de la información en la empresa, a través del método sugerido por el MSPI, análisis GAP (análisis de brechas de necesidades, a partir del estado actual y el estado objetivo).

Para el análisis, se tomó de referencia algunos de los numerales de la NTC-ISO/IEC 27001 (los criterios de selección de los numerales son de acuerdo con la expectativa actual de la empresa en el SGSI: A6 al A14).

Este análisis se realizó por medio de la observación, pruebas y entrevistas realizadas directamente con los empleados en sus estaciones de trabajo.

**Tabla 1**

*Análisis de brechas de necesidades, a partir del estado actual y el estado objetivo*

| | ITEM | CRITERIOS | HALLAZGOS | CUMPLIMIENTO INICIAL | CUMPLIMIENTO NIVEL INICIAL | Nivel Esperado |
|---|---|---|---|---|---|---|
| 1 | **A6. Organización interna de la seguridad y privacidad de la información** | 1). No existe objetivos de control, , políticas, procesos y procedimientos para la seguridad de la información, pero los directivos reconocen la necesidad, =20.<br>2). Existe un modelo de seguridad y privacidad de la información, con compromiso gerencial y definición de responsables, pero, no se han identificado los riesgos relacionados con las partes externas, = 60.<br>3). existe un modelo de seguridad y privacidad de la información por escrito con compromiso gerencial, con el reconocimiento de los riesgos relacionados con las partes externas para su desarrollo, sin haberse socializado y sin desarrollo =70.<br>4). El modelo de seguridad de la información está en desarrollo, =100 | Los directivos han identificado incidentes en la información, que los ha llevado a reconocer la necesidad de implementar un modelo.<br><br>La empresa no cuenta con un modelo de seguridad y privacidad de la información.<br><br>No se cuenta con el reconocimiento de los riesgos relacionados con las partes externas. | 20 | Muy Bajo | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | **A7. Gestión de activos** | 1). Los activos NO están identificados, por lo tanto, no hay relación con propietarios de activos ni uso aceptable del mismo =20<br>2). Los activos están identificados, pero no hay relación con propietario del activo o uso aceptable del activo = 40.<br>3). Existe un inventario de activos de información física y lógica, documentado y firmado por la alta dirección = 60.<br>3) Si se revisa y monitorean periódicamente los activos de información, y estos detallan la relación con propietarios de activos ni uso aceptable del mismo = 100. | Actualmente la empresa tiene un inventario de información física, con monitoreo periódicos y programación de mantenimientos. Es de conocimiento por la dirección.<br>No se lleva inventario de información lógica, propiedad de los activos, uso aceptable de los activos, ni de mantenimientos y/o actualizaciones. | 20 | Muy Bajo | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 | **A8. Seguridad de los recursos humanos** | 1). No están definidos los roles y responsabilidades en la seguridad y confidencialidad de la información, no están definidas en la relación contra actual en el contrato de trabajo, no se realiza control de información en terminación de contrato, =20.<br>2). Están definidos los roles y responsabilidades en la seguridad y confidencialidad de la información, pero no están definidas en la relación contra actual en el contrato de trabajo o no se realiza control de información ante terminación de contrato, =40.<br>3). Están definidos los roles y responsabilidades en la seguridad y confidencialidad de la información, están definidas en la relación contra actual en el contrato de trabajo y realiza control de información en terminación de contrato, =80.<br>4). Están definidos los roles y responsabilidades en la seguridad y confidencialidad de la información, están definidas en la relación contra actual en el contrato de trabajo, se realiza cumplimiento de devolución de activos y retiro de derechos de acceso, al finalizar la relación laboral=100. | Actualmente la empresa no ha definido el nivel de responsabilidad por la información, por lo que no hace parte del contrato o de la inducción al cargo. | 20 | Bajo | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | **Educación, formación y concientización sobre la seguridad de la información** | 1). Los trabajadores NO han recibido conocimiento y se han diseñado programas de sensibilización y capacitación = 40<br>2). Los trabajadores tienen conocimiento y los programas de capacitación, están aprobados y documentados, por la alta Dirección, = 60<br>3). Se ha desarrollado el programa de capacitación, aprobados por la alta Dirección, = 100 | No existe política de seguridad y privacidad de la información.<br><br>No se evidencia plan de Educación, formación y concientización sobre la seguridad de la información.<br><br>De acuerdo a la recolección de información, por medio de encuesta a los usuarios, la empresa realiza capacitaciones sobre seguridad y privacidad de la información, sin embargo, los comportamientos no reflejan una conciencia de seguridad. | 40 | Bajo | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | **A9. Seguridad física y del entorno** | 1). La empresa NO tiene definido áreas seguras: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización, así como tampoco cuenta con acciones para la seguridad de los equipos como seguridad de suministro, mmtt de equipos y retiro o desecho de equipos, =20.<br>2). La empresa cuenta con seguridad física en oficinas, controles de acceso a áreas autorizadas y personal no autorizado, sin embargo, los controles de seguridad de los equipos son deficientes (seguridad de suministro, mmtt de equipos y retiro o desecho de equipos), =40.<br>3). La empresa cuenta con controles de seguridad física y seguridad de los equipos, pero no lo suficientes (si falta alguno: áreas seguras evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización, seguridad de suministro, mmtt de equipos y retiro o desecho de equipos) =60<br>4).La empresa cuenta con controles de seguridad física y seguridad de los equipos y son suficientes (áreas seguras evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización, seguridad de suministro, mmtt de equipos y retiro o desecho de equipos), =100 | La empresa cuenta con acciones para las áreas seguras.<br>La empresa cuenta con acciones para la seguridad de los equipos, pero no son suficientes.<br>Cuenta con UPS (15 minutos) para todos los equipos, mantenimiento trimestral de los equipos.<br>No se llevan controles para reutilización de equipos o para retiro y desecho de equipos. | 60 | Medio | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | **A10. Gestión de comunicaciones y operaciones.** | 1). NO se cuenta con procedimientos del negocio, con procedimiento de gestión del cambio, respaldo de la información, controles de intercambio de información, sistema de comercio electrónico e integridad de información de acceso público, =20.<br>2). La empresa realiza por lo menos 3 de acciones detalladas en el numeral 1, =40.<br>3). La empresa realiza por lo menos 5 de las acciones detalladas en el numeral 1, =70.<br>4). La empresa realiza TODAS las acciones del numeral 1, =90.<br>5). La empresa da cumplimiento de controles especificados en el literal A.10 de la NTC/ISO/IEC 17001:2006, =100 | La empresa cuenta con procedimiento en casi todos los negocios, con respaldo de la información y sistemas de control de comercio electrónico. | 40 | Bajo | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | **A.12 Adquisición, desarrollo y mantenimiento de sistemas de información** | 1). La empresa no cuenta con un análisis y especificación de<br>los requisitos de seguridad para nuevos sistemas de información, valoración de vulnerabilidad, no cuenta con controles para instalación de nuevas aplicaciones y/o software, no se cuenta con control para asegurar que las aplicaciones críticas para el negocio se revisen y sometan a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización, =0.<br>2). La empresa realiza por lo menos 1 acción detalladas en el numeral 1, =20.<br>3). La empresa realiza por lo menos 2 de las acciones detalladas en el numeral 1, =40.<br>4). La empresa realiza por lo menos 3 de las acciones detalladas en el numeral 1, =60.<br>5). La empresa da cumplimiento a todas las acciones del numeral 1, =100 | De acuerdo a información recolectada en encuesta aplicada a los usuarios, tienen la libertad y posibilidad de instalar software o aplicativos sin restricciones de seguridad o permisos. | 0 | Bajo | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8 | **A.13 Gestión de incidentes de seguridad de la información** | 1). No se cuenta con un reporte sobre los eventos y las debilidades de la seguridad de la información, para la gestión de los incidentes y las mejoras no se cuenta con un responsable o procedimiento de acción y no se hace recolección de evidencias para las acciones disciplinarias o correctivas pertinentes, =0.<br>2). La empresa realiza 1 de las acciones del numeral 1, =20.<br>3). La empresa realiza 2 de las acciones del numeral 1, =60.<br>4). La empresa realiza todas las acciones del numeral 1, =100 | El usuario tiene posibilidad de reportar eventos o debilidades de la información, por medio de mecanismos formales o informales de comunicación. El usuario no tiene el conocimiento para identificar que evento podría llegar a considerarse una debilidad en la seguridad de la información. | 0 | Bajo | 100% |
| 9 | **A.14 Gestión de la continuidad del negocio** | 1). La empresa no cuenta con un proceso de gestión y continuidad del negocio, =0<br>2). La empresa cuenta con un proceso de gestión y continuidad del negocio e incluye la seguridad de la información, =80.<br>3). Dentro del proceso de gestión y continuidad del negocio que contempla la seguridad de la información, la empresa cuenta con identificación de eventos vulnerables, planes para mantener, recuperar y asegurar la información después de una interrupción o falla, =100. | La empresa no cuenta con proceso de gestión y continuidad del negocio. | 0 | Bajo | 100% |

*Nota*. En esta tabla se muestra el análisis de brechas de necesidades.

***Encuesta***

Se procedió con realizar una encuesta a los empleados de la empresa de manera online, para conocer el nivel de vulnerabilidad referente a la seguridad y privacidad de la información.

Para contar con fuentes primarias de información, se realizó un cuestionario sobre seguridad de la información (Ver Tabla 2), el cual permitió conocer la percepción y los comportamientos de las personas sobre los numerales a considerar en el proyecto.

Como se describe a continuación, el cuestionario consta de 25 preguntas, agrupadas:

**Tabla 2**

*Cuestionario sobre seguridad de la información*

| **Organización interna de la seguridad y privacidad de la información** |
|---|
| 1. ¿Accidentalmente ha sufrido pérdida de información en su puesto trabajo? |
| 4. Cuando se ausenta de su puesto de trabajo, ¿Su computador se queda prendido? |
| 7. Al ausentarse de su puesto de trabajo y este prendido su computador ¿cierra usted su sesión? |
| 20. ¿Su contraseña tiene como caracteres nombres de hijos, esposo, padres, mascotas, etc.? |
| 25. ¿Guarda su trabajo y cierra la aplicación cuando va a estar ausente? |
| **Gestión de comunicaciones y operaciones** |
| 2. ¿Alguna vez ha insertado un USB Memory en su puesto de trabajo? |
| 6. ¿Ha grabado información en su puesto de trabajo desde algún dispositivo de almacenamiento? |
| 12. ¿Ha llevado archivos digitales para terminar en su casa por falta de tiempo? |
| 13. ¿Tiene su ordenador información personal como fotos, videos, música, etc.? |
| 19. ¿Ha llevado archivos o documentos informáticos fuera de la empresa en USB Memory, CD, etc.? |
| 23. ¿Ha enviado archivos de la empresa desde su Hotmail o Gmail? |
| 24. ¿Tiene acceso a internet en su puesto de trabajo? |

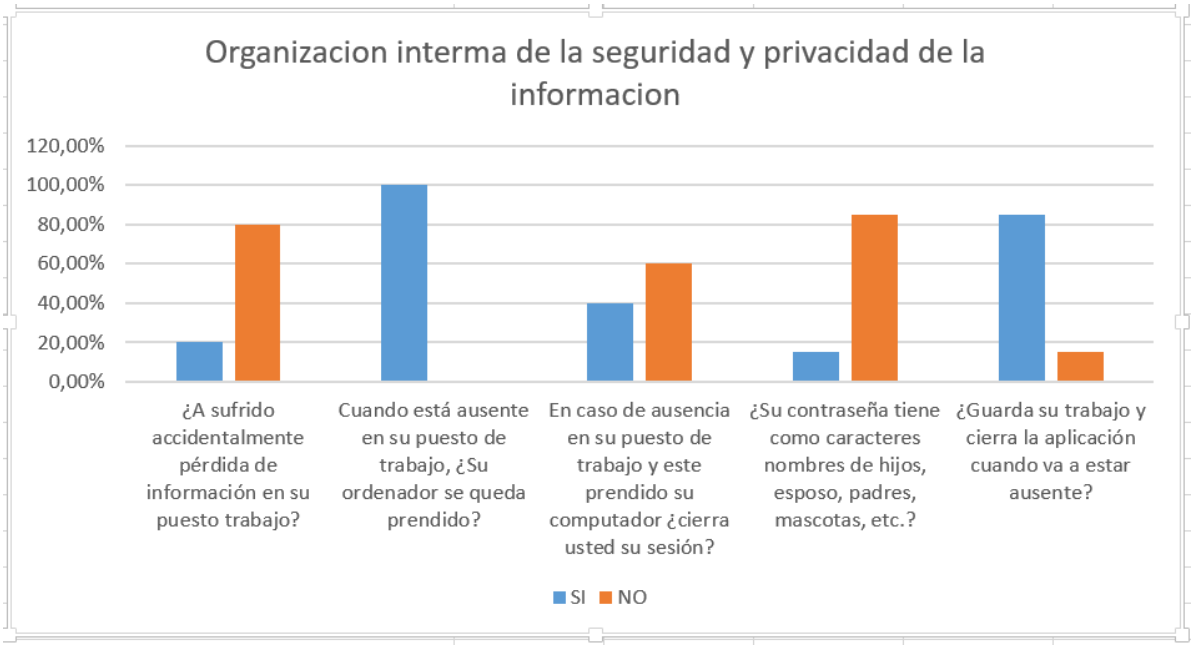
| **Educación** |
| --- |
| 3. ¿Conoce usted el término de encriptación de archivos? |
| 8. Cuando se instala un programa nuevo ¿Existe su debida capacitación? |
| 9. ¿Usted cree que la información dentro de la empresa está segura? |
| 18. ¿Ha tenido alguna capacitación para el mejor uso de las aplicaciones de su computadora, con el objetivo de mejorar su trabajo diario? |
| **Seguridad de los recursos humanos** |
| 5. ¿Ha instalado cualquier tipo de programa en su puesto de trabajo? |
| 16. ¿Ha intentado arreglar su computadora por su propia cuenta? |
| 10. ¿Ha realizado alguna vez un cambio de clave en su computadora? |
| 17. A parte de usted ¿Alguna otra persona conoce su contraseña de acceso a su computador? |
| **Adquisición, desarrollo y mantenimiento** |
| 14. ¿Se realiza el mantenimiento de su computador mensualmente? |
| 15. ¿Alguna vez se ha activado advertencias de antivirus? |
| 22. ¿Se ha instalado alguna aplicación para el mejor manejo de la información? |
| **Gestión de incidentes** |
| 11. ¿Se ha desconectado su computadora por apagones? |
| 21. ¿Ha perdido información por apagones? |

*Nota*. En esta tabla se muestra que los resultados permiten ver comportamiento vulnerable en cuanto a la confidencialidad, integridad y disponibilidad de la información, como se muestra a continuación:

**Tabla 3**

*Comportamientos en cuanto a organización interna de la seguridad y privacidad de la Información*

| **organización interna de la seguridad y privacidad de la información** | | |
|---|---|---|
| | **SI** | **NO** |
| 1. ¿A sufrido accidentalmente pérdida de información en su puesto trabajo? | 20% | 80% |
| 4. Cuando está ausente en su puesto de trabajo, ¿Su ordenador se queda prendido? | 100% | 0% |
| 7. En caso de ausencia en su puesto de trabajo y este prendido su computador ¿cierra usted su sesión? | 40% | 60% |
| 20. ¿Su contraseña tiene como caracteres nombres de hijos, esposo, padres, mascotas, etc.? | 15% | 85% |
| 25. ¿Guarda su trabajo y cierra la aplicación cuando va a estar ausente? | 85% | 15% |



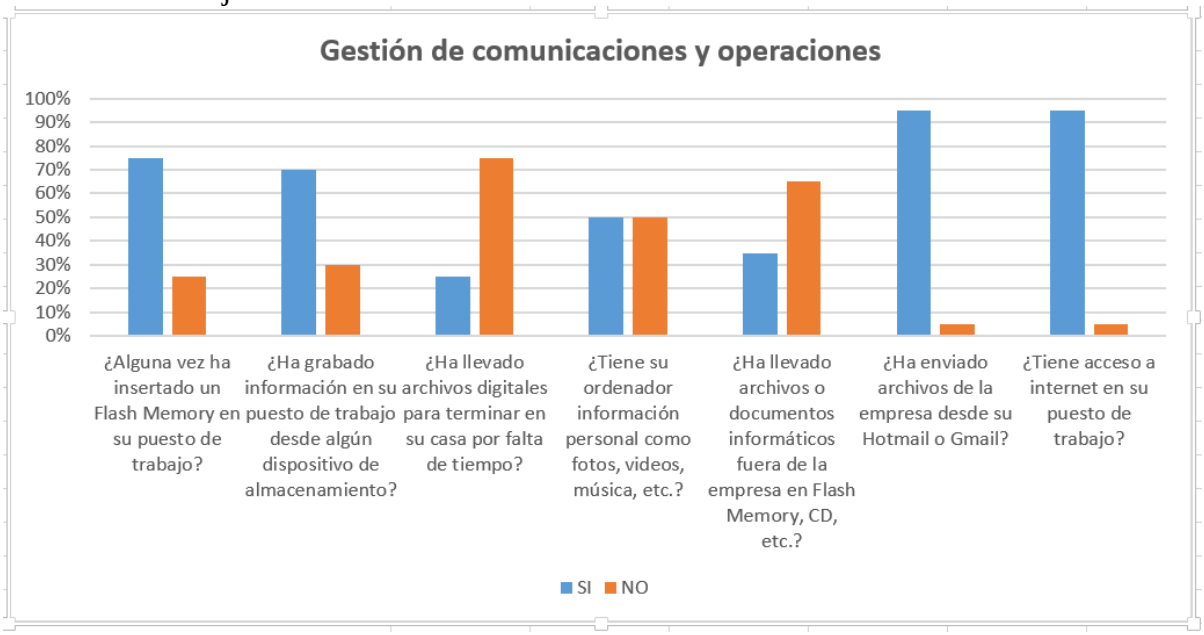

*Nota.* En esta tabla e imágenes de barras se muestra que las respuestas positivas a las preguntas N°1, 4, 20 y 25, reflejan comportamientos de riesgo para la seguridad y privacidad de la información; en 3 de 4 la gran mayoría de las personas (más del 50%) la respuesta fue "si". Por otro lado, en la pregunta N°7 la respuesta negativa, representa vulnerabilidad en la seguridad.

**Tabla 4**

*Gestión de comunicaciones y operaciones*

| **Gestión de comunicaciones y operaciones** | | |
|---|---|---|
| | **SI** | **NO** |
| 2. ¿Alguna vez ha insertado un Flash Memory en su puesto de trabajo? | 75% | 25% |
| 6. ¿Ha grabado información en su puesto de trabajo desde algún dispositivo de almacenamiento? | 70% | 30% |
| 12. ¿Ha llevado archivos digitales para terminar en su casa por falta de tiempo? | 25% | 75% |
| 13. ¿Tiene su ordenador información personal como fotos, videos, música, etc.? | 50% | 50% |

| | | |
|---|---|---|
| 19. ¿Ha llevado archivos o documentos informáticos fuera de la empresa en Flash Memory, CD, etc.? | 35% | 65% |
| 23. ¿Ha enviado archivos de la empresa desde su Hotmail o Gmail? | 95% | 5% |
| 24. ¿Tiene acceso a internet en su puesto de trabajo? | 95% | 5% |




*Nota*. En esta tabla e imágenes de barras se muestra en cuanto a las respuestas del trabajador en la gestión de comunicaciones y operaciones, se encuentra que el 75% de la población ha insertado flash memory, el 70% ha grabado información en algún dispositivo de almacenamiento, el 50% tiene en su ordenador información personal, el 95% se ha enviado archivos desde su correo personal y el 95% tiene acceso a internet en su puesto de trabajo. Es decir, más del 50% realizan acciones que ponen en riesgo la información en cuanto a la confidencialidad, integridad y disponibilidad de la información. Por otra parte, el 25% se ha llevado información en archivos digitales para su casa y el 35% se ha llevado archivos o documentos de forma digital fuera de la empresa.

**Tabla 5**

*Educación y formación*

| Educación y formación | | |
|---|---|---|
| | **SI** | **NO** |
| 3. ¿Conoce usted el término de encriptación de archivos? | 75% | 25% |
| 8. Cuando se instala un programa nuevo ¿Existe su debida capacitación? | 60% | 40% |
| 9. ¿Usted cree que la información dentro de la empresa está segura? | 100% | 0% |
| 18. ¿Ha tenido alguna capacitación para el mejor uso de las aplicaciones de su computadora, con el objetivo de mejorar su trabajo diario? | 75% | 25% |

*Nota*. En esta tabla se muestra que el 75% de los trabajadores manifiesta conocer los términos de encriptación de archivos, el 60% ha recibido capacitación ante la instalación y uso de nuevos programas, el 100% considera que la información es segura y el 75% ha recibido capacitación sobre el uso de aplicaciones para su trabajo. Las respuestas positivas en educación y formación reflejan protección en cuanto a la disponibilidad, integridad y confidencialidad de la información.

**Tabla 6**

*Seguridad de recursos humanos*

| Seguridad de los recursos humanos | | |
|---|---|---|
| | **SI** | **NO** |

| | | |
|---|---|---|
| 5. ¿Ha instalado cualquier tipo de programa en su puesto de trabajo? | 20% | 80% |
| 16. ¿Ha intentado arreglar su computadora por su propia cuenta? | 5% | 95% |
| 10. ¿Ha realizado alguna vez un cambio de clave en su computadora? | 45% | 55% |
| 17. A parte de usted ¿Alguna otra persona conoce su contraseña de acceso a su computador? | 10% | 90% |

*Nota*. En esta tabla se muestra que el 20% de los trabajadores ha instalado algún tipo de programa en su ordenador, el 5% ha intentado arreglar su computador por su propia cuenta, el 10% manifiesta que aparte de él, otra persona conoce la clave de acceso a su computadora. Las respuestas positivas son favorables para la seguridad de la información. Por otro lado, el 45% de los trabajadores ha cambiado su clave de usuario, siendo la respuesta positiva a la pregunta N°10 favorable para la seguridad de la información.

**Tabla 7**

*Adquisición, desarrollo y mantenimiento*

| **Adquisición, desarrollo y mantenimiento** | | |
|---|---|---|
| | **SI** | **NO** |
| 14. ¿Se realiza el mantenimiento de su computador mensualmente? | 85% | 15% |
| 15. ¿Alguna vez se ha activado advertencias de antivirus? | 65% | 35% |

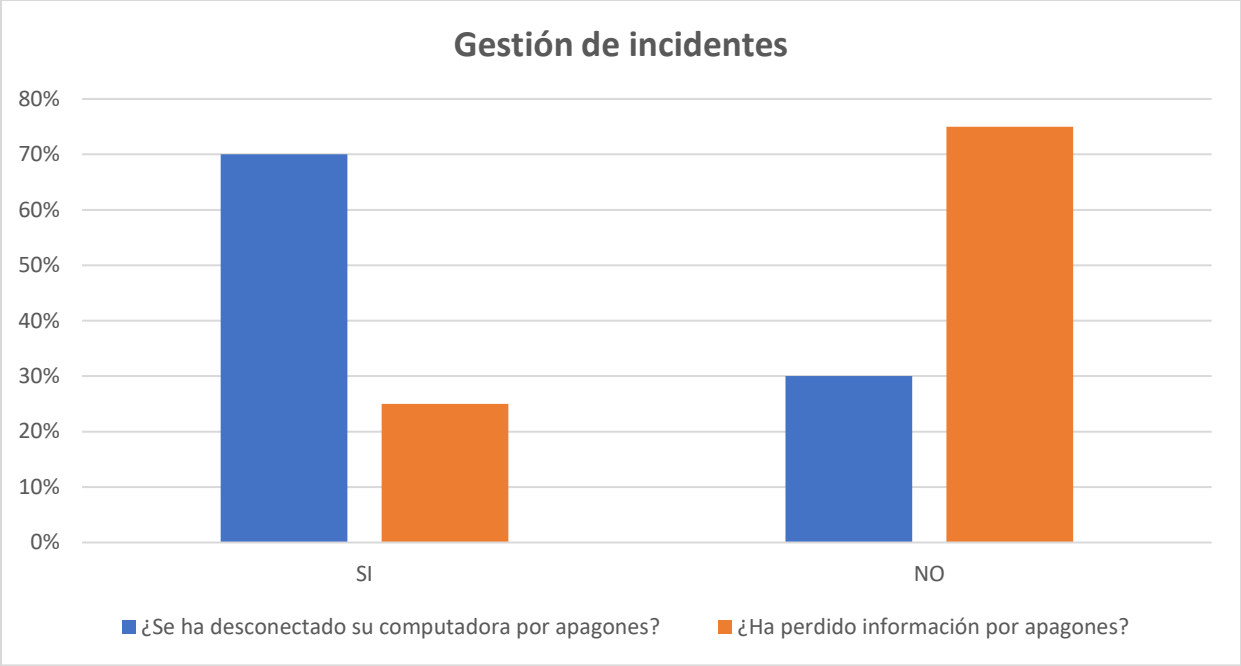
| | | |
|---|---|---|
| 22. ¿Se ha instalado alguna aplicación para el mejor manejo de la información? | 70% | 30% |

*Nota*. En esta tabla se muestra que el 85% de los trabajadores responde que mensualmente se realiza mantenimiento a su ordenador, el 65% ha tenido activación de advertencia de antivirus y el 70% afirma que en su ordenador se ha realizado instalación de aplicaciones para el mejor manejo de la información. Las respuestas positivas a las 3 preguntas son favorables para la seguridad y la privacidad de la información.

**Tabla 8**

*Gestión de incidentes*

| **Gestión de incidentes** | | |
|---|---|---|
| | **SI** | **NO** |
| 11. ¿Se ha desconectado su computadora por apagones? | 70% | 30% |
| 21. ¿Ha perdido información por apagones? | 25% | 75% |




*Nota*. En esta tabla e imágenes de barras se muestra que el 70% de los trabajadores ha respondido que ante apagones el computador se ha desconectado y el 25% ha tenido perdida de información por apagones. Las respuestas positivas a las 2 preguntas reflejan vulnerabilidad ante la seguridad y privacidad de la información.

**Realizar la planificación del sistema de seguridad de la empresa que satisfaga las necesidades de seguridad y privacidad de la información.**

***Fase 2: Planificación***

Esta etapa, permite a partir de la planeación, disponer de recursos y presupuesto para las actividades que se llevarán a cabo referente con el modelo MSPI, acorde a las expectativas actuales del negocio y sus partes interesadas.

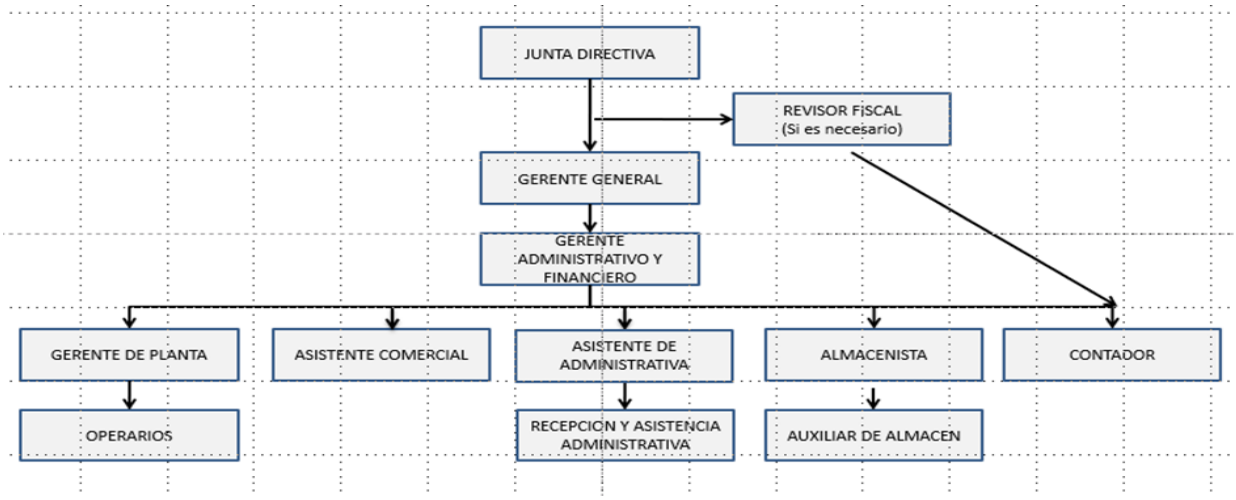
Para dar cumplimiento a la fase, es necesario reconocer el contexto de la empresa, su necesidad y expectativa, el alcance de un modelo en la seguridad y privacidad de la información, suscitar un compromiso de gestionar las acciones para la seguridad y privacidad de la información desde el liderazgo, definir roles y responsabilidades, identificación de los activos de la información, valorar el riesgo en la seguridad informática y finalmente, proponer un plan de tratamiento de los riesgos de seguridad de la información.

**Contexto.** INTERNATIONAL PROTECTION, es una compañía dedicada a la generación de sistemas de seguridad y blindaje vehicular, Hoy por hoy tiene 30 colaboradores entre las áreas de dirección, administración y operación, quienes utilizan de forma frecuente la información para consultar datos, que se usan como base para el cumplimiento de sus actividades diarias.

La estructura organizacional es vertical, con responsables de procesos y personas de forma directa.

**Figura 2**

*Estructura organizacional International Protection*




*Nota.* En esta figura se muestra el organigrama de la empresa International Protection.

Se visualiza en el 2027 consolidada como la empresa líder de Blindaje Vehicular en la Región Caribe Colombiana e iniciando una fuerte penetración en el mercado internacional, garantizando siempre la más alta calidad en los servicios y procesos.

Respondiendo a su proceso de calidad, declara los siguientes objetivos de calidad:

- Mantener un SGSI encaminado al mejoramiento continuo de nuestros procesos.
- Gestionar la adquisición y mantenimiento de la más avanzada tecnología en maquinaria, materia prima y procesos relacionados con la actividad.
- Mantener un recurso humano altamente calificado para el óptimo desempeño de sus actividades.
- Aumentar la satisfacción de nuestros clientes cumpliendo con las necesidades y requerimientos establecidos.
- Mantener una infraestructura óptima para el cumplimiento de las actividades

generando un ambiente de trabajo adecuado bajo estándares de seguridad.

**Necesidades y expectativas.**

**Tabla 9**

*Necesidades y expectativas*

| **Parte** | **Influencia** | **Expectativas y necesidades** |
|---|---|---|
| Junta Directiva | - Capacidad de decisiones en todos los procesos de la organización.<br>- Disponen de todos los recursos de la empresa.<br>- Acceso a toda la información de la organización. | – confidencialidad, integridad y disponibilidad de la información.<br>– Cumplimiento legal.<br>– Mantener el Prestigio y reputación.<br>– Sostenibilidad.<br>– Uso eficiente de los recursos |
| Gerencias | - Toman decisiones en todos los procesos de la organización.<br>- En promover acciones para la seguridad y privacidad de la información.<br>- Disponer de recursos para las acciones MSPI.<br>- Habilitar los recursos y procesos para la aplicación del MSPI. | - Acciones del MSPI fáciles y amigables a la operación.<br>- Acciones para garantizar la confidencialidad, integridad y disponibilidad de la información que custodian y administran<br>- Uso eficiente de los recursos<br>- Que las acciones del MSPI contribuya a los SGI.<br>- Que el MSPI, pueda ser un atractivo para fidelización y atracción de clientes. |
| Trabajadores | - Responsabilidad en accionar el MSPI, por lo tanto, pueden habilitar o invalidar | - |

| | | |
|---|---|---|
| | las acciones del MSPI | |
| Clientes | - Solicitud de información de información reservada o clasificada. | - Custodia y manejo de información de forma segura y respetuosa. |

*Nota*. En esta tabla se muestra las necesidades y expectativas de las partes interesadas en International Protection, en el MSPI.

**Compromiso.**

**Política.** Para International Protection, la seguridad de la información disminuye el impacto no deseado, que puede ser generado de manera sistemática. Por lo tanto, aspira controlar el nivel de exposición que garantice la integridad, confidencialidad y la disponibilidad, conforme a los requerimientos de los diferentes grupos de interés.

- La política aplica a los trabajadores, proveedores, aprendices y practicantes, y los principios sobre los que se basa están determinadas por los siguientes indicios:
    - Disminuir el máximo riesgo en las funciones.
    - Efectuar el acatamiento de los principios de seguridad de la información.
    - Realizar el acatamiento de los principios de las funciones administrativas.
    - Conservar la confidencia de clientes, socios y empleados.
    - Apoyo en las innovaciones tecnológicas.
    - Salvaguardar todo lo relacionado a los activos tecnológicos.
    - Constituir las políticas, procedimientos e instructivos en materia de seguridad de la información.
    - Fortificar el compromiso de seguridad de la información en los trabajadores, terceros, practicantes y clientes

- Garantías para la continuidad del negocio frente a incidentes.
- Se declara que todas las partes interesadas del negocio son responsables del acatamiento de la presente política, y que su incumplimiento podría tener como consecuencia la aplicación de actos administrativos.

**Roles y responsabilidades.**

**Tabla 10**

*Roles y responsabilidades*

| CARGO | AUTORIDAD | FUNCIONES |
|---|---|---|
| GERENTE | Puede y debe tomar decisiones de todo tipo en todos los procesos de la organización | – Ejecución y celebración de todo acto entendido dentro del objetivo social.<br>– Formulación, dirección, evaluación y control de todo lo concerniente al afianzamiento y que se cumplan las políticas y estrategias generales de la empresa estableciendo objetivos y metas específicas.<br>– Efectuar por mandato de la Junta Directiva los planes, programas y proyectos requeridos para el desarrollo armónico de la organización. Asegurar, evaluar y negociar títulos valores.<br>– Custodia y administra información reservada. |
| GERENTE ADMINISTRATIVO Y FINANCIERO | Puede y debe tomar decisiones de todo tipo en todos los procesos de la organización, especialmente en todos los procesos de apoyo y el mejoramiento continuo | – Analizar los aspectos económicos en la toma de decisiones.<br>– Anualmente generar y monitorear el presupuesto de ventas.<br>– Análisis de la cantidad de inversión necesaria para alcanzar las ventas esperadas.<br>– Optar por las fuentes y representaciones alternativas de fondos para la financiación en la toma de decisiones de inversiones establecidas por la Junta Directiva.<br>– Custodia y administra información reservada |

| | | |
|---|---|---|
| GERENTE DE PLANTA | Sus decisiones deben estar autorizadas por la gerencia. sin embargo, puede tomar decisiones autónomas en temas referentes al proceso de prestación de servicios. | – Mantener al día el archivo de seguimiento compartido en lo que le corresponde.<br>– Participar, bajo el mando del gerente, en la programación semanal de las actividades a realizar para la prestación del servicio de blindaje y mantenimiento<br>– Asignación de personal, en conjunto con gerencia, para las tareas a realizar a cada vehículo.<br>– Responsable de solucionar un servicio técnico, en el momento en que un vehículo ingrese por garantía del servicio.<br>– Supervisa constantemente el proceso de prestación del servicio incluyendo los procesos de Recepción y Diagnostico, Desarme de vehículo, Blindaje del vehículo, Armado y Prueba de Ruta, según SGC.<br>– Custodia y administra información reservada. |
| ASISTENTE DE COMERCIAL | Sus decisiones deben estar autorizadas por la gerencia. | – Realizar las cotizaciones requeridas por gerencia y su respectivo seguimiento a clientes.<br>– Mantener al día los archivos de seguimiento de cotizaciones, estatus de reclamaciones,<br>– seguimiento compartido.<br>– Realizar las respectivas encuestas de satisfacción a clientes.<br>– Comunicación e informe constante con gerencia acerca de aspectos a mejorar según su criterio.<br>– Presentación personal impecable utilizando el uniforme proporcionado por INTERNATIONAL PROTECTION. |

| | | |
|---|---|---|
| | | - Custodia y administra información reservada |
| REVISOR FISCAL | Sus decisiones deben estar avaladas siempre por el gerente administrativo y financiero | - Llevar los libros y registros contables de la empresa.<br>- Diseñar, implantar y administrar sistemas de información.<br>- Elaboración de los informes sobre las condiciones presupuestales, financieras y contables de la organización.<br>- Ejecutar su profesión asistiendo con la gerencia en la consecución de sus obligaciones en lo presupuestal, financiera y contable. Realización de control de las gestiones y evaluaciones de control interno.<br>- Realiza la oportuna liquidación de impuestos, retenciones y demás obligaciones tributarias de la organización.<br>- Presentación de estados financieros a gerencia durante los primeros 15 días de cada mes. (Balance General, Estado de Resultado acumulado y del periodo con sus anexos)<br>- Conciliación de cuentas bancarias y caja.<br>- Custodia y administra información reservada |
| ALMACENISTA | Sus decisiones deben estar avaladas siempre por la gerencia | - Presentación personal impecable en todo momento utilizando los uniformes proporcionados por INTERNATIONAL PROTECTION.<br>- Realizar apertura y cierre oportuno diario siguiendo las pautas de seguridad y prevención establecidas por gerencia.<br>- Custodia y manejo del almacén de la empresa. |

| | | |
|---|---|---|
| | | - Realización, registro y control del ingreso y la salida de insumos y mercancías a almacén y la planta.<br>- Realizar informe detallado de insumos consumidos por vehículo y presentarlo a jefe de operaciones de manera oportuna.<br><br>- Recepción de todos los vehículos que ingresen a planta, diligenciando el formato adecuado donde queda registrado el estado del vehículo.<br>- Custodia y administra información pública clasificada. |
| CONTADOR | Sus decisiones deben estar avaladas siempre por el gerente administrativo y financiero | - Llevar libros, registros contables de la organización.<br>- Mantener el archivo de proveedores al día.<br>- Ejecutar su profesión asistiendo con la gerencia en la consecución de sus obligaciones en materia de presupuesto, financiamiento y contabilidad. Efectúa control de las gestiones y evaluaciones de control interno.<br>- Apoyado y supervisado por el REVISOR FISCAL, Realiza la oportuna liquidación de impuestos, retenciones y demás obligaciones tributarias de la organización.<br>- Custodia y administra información reservada. |
| ASISTENTE ADMINISTRATIVA | Sus decisiones deben estar avaladas siempre por la gerencia. sin embargo, puede tomar decisiones autónomas en el procedimiento de compras, tramites y cotizaciones | - Elaboración de órdenes de compra aprobadas por gerencia y su respectivo envío a proveedores, así como su seguimiento y verificación de recibo.<br>- Responsable de envío de órdenes de compra a proveedores y su seguimiento<br>- Apoyar a la Asistente comercial en la realización de cotizaciones de las empresas de terceros de acuerdo con el interés gerencial. |

| | | |
|---|---|---|
| | | - Atención de cafetería a clientes.<br>- Recepción y transferencia de llamadas telefónicas.<br>- Custodia y administra información pública clasificada. |
| RECEPCIONISTA / ASISTENTE ADMINISTRATIVA | Sus decisiones deben estar avaladas siempre por la gerencia. sin embargo, puede tomar decisiones autónomas en el envío y recibo de correspondencia, agendas, sistema de gestión de calidad | - Conservar en adecuado estado de servicio, presentación y funcionamiento el sitio de recepción.<br>- Apoya a la Asistente Administrativa en la gestión y procesos de compras.<br>- Atención de llamadas y transferencia por conmutador a su respectivo destinatario<br>- Apoya al jefe de operaciones en todo lo relacionado con el mantenimiento del SGC<br>- Contestación y registro de todas las llamadas entrantes a la empresa.<br>- Control, registro y seguimiento de entrada y salida de correspondencia. |
| OPERARIOS | Sus decisiones deben estar avaladas siempre por la gerencia | - La utilización, en todo instante, de los equipos de seguridad suministrados por la organización necesarios para la realización de las actividades diarias asignadas.<br>- Mantener siempre una presentación personal impecable utilizando los uniformes suministrados por INTERNATIONAL PROTECTION.<br>- Mantener en completa limpieza y aseo el área de trabajo una vez terminadas las labores. (Barrer o trapear el área según sea necesario). |

| | |
|---|---|
| | - Asistencia a capacitaciones coordinadas por gerencia que fomenten el conocimiento y habilidad necesarios para la ejecución de la prestación del servicio.<br>- Cumplir con las tareas asignadas por gerencia y jefe de planta en el tiempo establecido.<br>- Todas sus labores deben seguir los requisitos de calidad instaurados bajo la norma ISO 9001.<br>- Asistencia, en lo posible, a las actividades de bienestar y de recreo coordinadas por la empresa.<br>- Administra información pública clasificada. |

*Nota.* En esta tabla se muestra la autoridad, funciones y responsabilidades de las partes interesadas en International Protection, dentro del MSPI.

## Determinar los riesgos y definir las acciones para valorarlos precisando el plan de tratamiento sobre ellos.

### *Identificación de la información y la infraestructura*

Para identificar los activos de la empresa INTERNATIONAL PROTECTION, se utilizó la Guía N°5 para la Gestión y Clasificación de Activos de Información (MSPI - MINTICS).

**Tabla 11**

*Clasificación de activos*

| MARCA | PROCESADOR | MEMORIA | DISCO DURO | SISTEMA OPERATIVO | SERIAL | USUARIO | CUSTODIO | CARGO | UBICACIÓN | INFORMACIÓN |
|---|---|---|---|---|---|---|---|---|---|---|
| MAC | QUAD CORE I5 2.8 | 8 GB | 1 TB | MA COSX 10.16 | QP8460LPZE | CRISTIAN TARUD | CRISTIAN TARUD | GERENTE ADMINISTRATIVO | GERENCIA | CONFIDENCIAL |
| MAC | QUAD CORE I5 2.8 | 8 GB | 2 TB | MA COSX 10.16 | QP8470LPZE | CHRISTIAN CORONEL | CHRISTIAN CORONEL | GERENTE FINANCIERO | TALLER | CONFIDENCIAL |
| MAC | QUAD CORE I5 2.8 | 8 GB | 3 TB | MA COSX 10.16 | QP8480LPZE | JHONNY JANNE | JHONNY JANNE | GERENTE GENERAL | GERENCIA | CONFIDENCIAL |
| MAC | QUAD CORE I5 2.9 | 9 GB | 4 TB | MA COSX 10.17 | QP8490LPZE | AROLDO TINOCO | AROLDO TINOCO | GERENTE DE PLANTA | TALLER | CONFIDENCIAL |
| HP | CORE I3 8100 3.6 | 8 GB | 1 TB | WIN 10 | CNU5678932 | MANUEL CONTRERAS | MANUEL CONTRERAS | ASISTENTE PLANTA | TALLER | RESTRINGIDA |
| HP | CORE I3 8100 3.6 | 8 GB | 1 TB | WIN 10 | CNF5678933 | DIANA CLAVIJO | DIANA CLAVIJO | COMERCIAL | ADMINISTRATIVA | RESTRINGIDA |
| HP | CORE I3 8100 3.6 | 8 GB | 1 TB | WIN 10 | CNU5678934 | JUAN ESCORCIA | JUAN ESCORCIA | JEFE ALMACEN | ALMACEN | RESTRINGIDA |
| HP | CORE I3 8100 3.6 | 8 GB | 1 TB | WIN 10 | CNU5678935 | ELIANA ESCORCIA | ELIANA ESCORCIA | ASISTENTE ALMACEN | ALMACEN | RESTRINGIDA |
| HP | CORE I3 8100 3.6 | 8 GB | 1 TB | WIN 10 | CNU5678936 | FANOR ARRIETA | FANOR ARRIETA | ASISTENTE ALMACEN | ALMACEN | RESTRINGIDA |
| HP | CORE I3 8100 3.6 | 8 GB | 1 TB | WIN 10 | CNF5678937 | ETEMILDA RUEDA | ETEMILDA RUEDA | CONTADORA | ADMNINISTRATIVA | CONFIDENCIAL |
| HP | CORE I3 8100 3.6 | 8 GB | 1 TB | WIN 10 | CNU5678938 | MARTHA VARGAS | MARTHA VARGAS | ASISTENTE ADMINISTRATIVA | ADMINISTRATIVA | CONFIDENCIAL |
| HP | CORE J3060 2.4 | 4 GB | 500 GB | WIN 10 | CNU5678939 | JAYLING BURGOS | JAYLING BURGOS | RECEPCIONISTA | RECEPCION | INTERNA |
| HP | CORE J3060 2.4 | 4 GB | 500 GB | WIN 10 | CNU5678940 | ANGEL PEREZ | ANGEL PEREZ | ASITENTE PLANTA | TALLER | INTERNA |
| HP | CORE J3060 2.4 | 4 GB | 500 GB | WIN 10 | CNU5678941 | JESUS CORONADO | JESUS CORONADO | OPERADOR | TALLER | INTERNA |
| HP | CORE J3060 2.4 | 4 GB | 500 GB | WIN 10 | CNU5678942 | LEONEL ARRIETA | LEONEL ARRIETA | OPERADOR | TALLER | INTERNA |

*Nota.* En esta tabla se muestra una descripción detallada de los activos informáticos.

**Tabla 12**

*Clasificación de activos de acuerdo con su nivel de seguridad*

| MARCA | PROCESADOR | SERIAL | CUSTODIO | UBICACIÓN | CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBIIDAD |
|---|---|---|---|---|---|---|---|
| MAC | QUAD CORE I5 2.8 | QP8460LPZE | CRISTIAN TARUD | GERENCIA | PUBLICA RESERVADA | ALTA | ALTA |
| MAC | QUAD CORE I5 2.8 | QP8470LPZE | CHRISTIAN CORONEL | TALLER | PUBLICA RESERVADA | ALTA | ALTA |
| MAC | QUAD CORE I5 2.8 | QP8480LPZE | JHONNY JANNE | GERENCIA | PUBLICA RESERVADA | ALTA | ALTA |
| MAC | QUAD CORE I5 2.9 | QP8490LPZE | AROLDO TINOCO | TALLER | PUBLICA RESERVADA | ALTA | ALTA |
| HP | CORE I3 8100 3.6 | CNU5678932 | MANUEL CONTRERAS | TALLER | PUBLICA CLASIFICADA | MEDIA | BAJA |
| HP | CORE I3 8100 3.6 | CNF5678933 | DIANA CLAVIJO | ADMINISTRATIVA | PUBLICA RESERVADA | MEDIA | BAJA |
| HP | CORE I3 8100 3.6 | CNU5678934 | JUAN ESCORCIA | ALMACEN | PUBLICA RESERVADA | ALTA | MEDIA |
| HP | CORE I3 8100 3.6 | CNU5678935 | ELIANA ESCORCIA | ALMACEN | PUBLICA CLASIFICADA | MEDIA | BAJA |
| HP | CORE I3 8100 3.6 | CNU5678936 | FANOR ARRIETA | ALMACEN | PUBLICA CLASIFICADA | MEDIA | BAJA |
| HP | CORE I3 8100 3.6 | CNF5678937 | ETEMILDA RUEDA | ADMNINISTRATIVA | PUBLICA RESERVADA | ALTA | ALTA |
| HP | CORE I3 8100 3.6 | CNU5678938 | MARTHA VARGAS | ADMINISTRATIVA | PUBLICA CLASIFICADA | MEDIA | MEDIA |
| HP | CORE J3060 2.4 | CNU5678939 | JAYLING BURGOS | RECEPCION | PUBLICA CLASIFICADA | MEDIA | BAJA |
| HP | CORE J3060 2.4 | CNU5678940 | ANGEL PEREZ | TALLER | PUBLICA CLASIFICADA | MEDIA | BAJA |
| HP | CORE J3060 2.4 | CNU5678941 | JESUS CORONADO | TALLER | PUBLICA CLASIFICADA | MEDIA | BAJA |
| HP | CORE J3060 2.4 | CNU5678942 | LEONEL ARRIETA | TALLER | PUBLICA CLASIFICADA | MEDIA | BAJA |

*Nota.* En esta tabla se muestra la clasificación de activos de acuerdo con su nivel de seguridad, por medio de la confidencialidad, integridad y continuidad.

**Valoración de los riesgos en la seguridad informática: amenazas, vulnerabilidades y riesgos puedan presentarse en los activos de la organización.**

Al realizar la investigación o análisis de riesgos permite comprobar los riesgos en que podría acontecer en la organización INTERNATIONAL PROTECTION, identificando los activos de la empresa, a su vez establecer a que tipos de amenazas se puede estar expuesto.

D= Deliberadas, A= Accidentales, E= Ambientales

**Tabla 13**

*Identificación de amenazas*

| TIPO | AMENAZA | ORIGEN |
|---|---|---|
| **Daño físico** | El Fuego | A |
| | El Agua | A/E |
| | Las contaminaciones | A |
| | Los Accidentes de importancia | A |
| | La destrucción de los equipos | A/E |
| | El Polvo, la corrosión | A/E |
| **Eventos naturales** | Los fenómenos climáticos | E |
| | Los fenómenos sísmicos | E |
| | Los fenómenos volcánicos | E |
| | Los fenómenos meteorológicos | E |
| | Las inundaciones | E |
| **Perdida de los servicios esenciales** | Las fallas en el sistema en el suministro de agua o aire condicionado | D/A/E |
| | La falla del suministro de energía | D/A/E |
| | Las fallas en dispositivos de telecomunicaciones | D/A/E |
| **Perturbación debida a la radiación** | Las radiaciones electromagnéticas | A/E |
| | Las radiaciones térmicas | A |
| | Los pulsos electromagnéticos | A/E |
| **Compromiso de la información** | Las interceptaciones de señales de interferencia comprometida | D |
| | Los espionajes remotos | D |
| | Los escucha encubierta | D |
| | Los hurtos de los medios o documentaciones | D |
| | Las recuperaciones de los medios para reciclar | D |
| | Las divulgaciones | D |
| | Información procedente de orígenes no confidenciales | D |

| | | |
|---|---|---|
| | Las manipulaciones con hardware | D |
| | Las manipulaciones con software | D |
| | Las detecciones de la posición | D |
| **Fallas técnicas** | Las fallas de los equipos | D/A |
| | El deficientemente funcionamiento de los dispositivos | A |
| | Las Saturaciones del sistema de información | A |
| | Los malos funcionamientos del software | A |
| | Los Incumplimientos en los mantenimientos del sistema de información o mantenimientos o programados | D/A |
| **Acciones no autorizadas** | La manipulación no autorizada de los equipos | D |
| | El uso no autorizado del equipo | D |
| | La utilización de softwares falsos o copiadas | D |
| | La corrupción de los datos | D |
| | El procesamiento ilegal de los datos | D |
| **Compromiso de las funciones** | Los errores en el uso | D |
| | Los abusos de los derechos | D |
| | La clasificación de derechos | D |
| | La negación de acciones | D |
| | El incumplimiento en la disponibilidad del personal | D |

*Nota.* En esta tabla se muestra la identificación de vulnerabilidades se realiza a partir de las amenazas, de acuerdo con la guía N°7, una vulnerabilidad que no tiene una amenaza puede no requerir de control.

A continuación, se identifica las vulnerabilidades.

**Tabla 14**

*Identificación de vulnerabilidades*

| TIPO DE ACTIVO | VULNERABILIDADES | AMENAZA |
|---|---|---|
| **HARDWARE** | Los mantenimientos son insuficientes/Instalaciones fallidas de los medios donde se almacenan | No programación de los mantenimientos de los sistemas de información |
| | Susceptible a la variación del voltaje | No provisión de energía y recarga a UPS |
| | El almacenamiento sin protecciones | Robos |

| | | |
|---|---|---|
| | La falta de atención en las disposiciones finales | Robos |
| | Las copias no controladas | Robos |
| **SOFTWARE** | Las asignaciones erradas de los derechos de acceso | Abuso de los derechos |
| | Las Disposiciones o reutilizaciones de los medios de guardado sin el borrado apropiado | Abuso de los derechos |
| | Los registros de las contraseñas sin protecciones | Falsificaciones de los derechos |
| | Las gestiones inadecuadas de las contraseñas | Falsificaciones de los derechos |
| | Las descargas y utilización no controlado de los softwares | Manipulaciones con software |
| | Las ausencias de copias de seguridad | Manipulaciones con software |
| **RED** | La conexión deficiente de los cables | Fallas de los equipos de telecomunicación. |
| | La construcción insegura de la red | Espionajes remotos |
| | Traspaso de contraseñas en claro | Espionajes remotos |
| | Las gestiones indebidas de la red (tolerancia a fallas en el enrutamiento) | Saturaciones del sistema de información |
| | Las interconexiones de la red pública sin seguridad | No autorización de uso |
| **PERSONAL** | Preparación escasa en seguridad | Errores |
| | La utilización incorrecta del hardware y software | Errores |
| | El desconocimiento referente a la seguridad | Errores |
| | La ausencia de los mecanismos de monitoreo | ilegal procesamiento de los datos |
| | La inexistencia de políticas para el uso adecuado de los medios de comunicaciones y mensajería. | No autorización de uso |

| | | |
|---|---|---|
| **LUGAR** | La utilización indebida o descuidado del control de acceso físico a las edificaciones y recintos | Espionajes remotos |
| | La red de energía inestable | Mal funcionamiento del equipo |
| **ORGANIZACIÓN** | Ausencia de procedimiento formal para el registro y retiro de usuarios | Abuso |
| | La ausencia de procesos formales para las revisiones de los derechos de acceso | Abuso |
| | La no existencia de auditorias | Abuso |
| | La ausencia de procedimientos para identificar y valorar los riesgos | Abuso |
| | La ausencia de procedimientos de control de cambios | Incumplimiento en el mantenimiento de los sistemas de información |
| | La no existencia de procesos y procedimientos formales para documentar el MSPI | Corrupción de datos |
| | La no existencia de políticas referente al uso de correo electrónico | Errores |
| | La ausencia de los procedimientos para el manejo de información clasificada | Errores |
| | La no existencia de responsabilidad en la seguridad de la información en la descripción de los cargos | Errores |
| | La inexistencia de mecanismos para monitorear las brechas en seguridad | Robo |

*Nota*. Una vez teniendo en cuenta la identificación de las amenazas y vulnerabilidades, se continua con la identificación de los riesgos por la probabilidad e impacto. La probabilidad es la posibilidad de ocurrencia del riesgo, teniendo en cuenta factores internos o externos de la organización y el impacto, se identifica como la consecuencia que puede tener la materialización del riesgo. Los criterios de identificación en la evaluación de probabilidad e impacto están definidos en el siguiente gráfico: Matriz de Calificaciones, Evaluaciones y respuestas a los

Riesgos (MSPI, Mintics, Guía N°7)

**Figura 3**

*Matriz de calificación, evaluación y respuesta a los riesgos*

*Ilustración 3 "Matriz de Calificación, Evaluación y respuesta a los Riesgos"*

| PROBABILIDAD | IMPACTO | | | | |
|---|---|---|---|---|---|
| | Insignificante (1) | Menor (2) | Moderado (3) | Mayor (4) | Catastrófico (5) |
| Raro (1) | B | B | M | A | A |
| Improbable (2) | B | B | M | A | E |
| Posible (3) | B | M | A | E | E |
| Probable (4) | M | A | A | E | E |
| Casi Seguro (5) | A | A | E | E | E |

**B: Zona de riesgo Baja:** Asumir el riesgo
**M: Zona de riesgo *Moderada*:** Asumir el riesgo, Reducir el riesgo
**A: Zona de riesgo *Alta*:** Reducir el riesgo, Evitar, Compartir o Transferir
**E: Zona de riesgo *Extrema*:** Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

*Nota.* En esta figura se muestra la matriz de calificación, evaluación y respuesta a los riesgos (MSPI, 2016, Guía de gestión de riesgos, pág.37)

**Tabla 15**

*Análisis del riesgo*

**Análisis del riesgo**

Objetivo: Proporcionar gestión oportuna a las necesidades y expectativas, dentro de una cultura de servicio y en cumplimiento legal

| RIESGO | CALIFICACIÓN | | Tipo de impacto | Evaluación | Medidas de respuesta |
|---|---|---|---|---|---|
| | Probabilidad | Impacto | | Zona de Riesgo | |
| Los mantenimientos insuficientes | 4 | 3 | No programación de mantenimiento del sistema de información | Alta | Reducción del riesgo, evitar, compartir o transformar |
| Las variaciones del voltaje | 3 | 2 | Pérdida de energía y recarga a UPS | Moderada | Asumirse el Riesgo, Reducción del riesgo |
| Los almacenamientos sin ninguna protección | 4 | 4 | Robos medios o documentos | Extrema | Reducción del riesgo, evitar, compartir o transformar |
| El descuido en la disposición final | 4 | 2 | Robos medios o documentos | Alta | Reducción del riesgo, evitar, compartir o transformar |
| Copia no controlada | 4 | 3 | Robos medios o documentos | Alta | Reducción del riesgo, evitar, compartir o transformar |
| Asignaciones erradas de los derechos de acceso | 3 | 2 | Abusar derechos | Moderada | Asumirse el Riesgo, reducir el riesgo |
| Las disposiciones o reutilizaciones de los medios de almacenamiento sin borrado adecuado | 4 | 2 | Abusar derechos | Alta | Reducción del riesgo, evitar, compartir o transformar |

| | | | | | |
|---|---|---|---|---|---|
| Registros de contraseñas sin protección | 2 | 3 | Derechos falsificados | Moderada | Asumirse el Riesgo, reducir el riesgo |
| Deficiente gestión de las contraseñas | 2 | 3 | Derechos falsificados | Moderada | Asumirse el Riesgo, reducir el riesgo |
| La descarga y el uso no controlado de software | 4 | 4 | Manipulaciones del software | Extrema | Reducción del riesgo, evitar, compartir o transformar |
| No se tienen copias de respaldo | 1 | 4 | Manipulaciones del software | Alta | Reducción del riesgo, evitar, compartir o transformar |
| Conexiones deficientes de los cables | 3 | 2 | Fallas del dispositivo de comunicaciones | Moderada | Asumirse el Riesgo, reducir el riesgo |
| Arquitectura insegura de la red | 3 | 4 | Espionajes remotos | Extrema | Reducción del riesgo, evitar, compartir o transformar |
| La transferencia de contraseñas | 2 | 3 | Espionajes remotos | Moderada | Asumirse el Riesgo, reducir el riesgo |
| La inadecuada gestión de la red (fallas de enrutamiento) | 1 | 3 | Saturaciones de los sistemas de información | Moderada | Asumirse el Riesgo, reducir el riesgo |
| La conexión de red pública sin ninguna protección | 1 | 2 | No autorizado de uso del equipo | Baja | Asumirse el Riesgo |
| El insuficiente entrenamiento en seguridad | 4 | 3 | Error en el uso | Extrema | Reducción del riesgo, evitar, compartir o transformar |

| | | | | | |
|---|---|---|---|---|---|
| El uso inadecuado del software y hardware | 3 | 4 | Errores de uso | Extrema | Reducción del riesgo, evitar, compartir o transformar |
| El no conocimiento acerca de la seguridad | 3 | 3 | Errores de uso | Alta | Reducción del riesgo, evitar, compartir o transformar |
| No contar con mecanismos para monitorear | 2 | 2 | Procesamiento de los datos ilegalmente | Baja | Asumirse el Riesgo |
| No contar con políticas para el uso apropiado de los medios de comunicaciones y mensajería | 4 | 3 | No autorizado de uso del equipo | Alta | Reducción del riesgo, evitar, compartir o transformar |
| Descuido en el control de acceso físico a las edificaciones y los recintos | 2 | 2 | Espionaje remoto | Baja | Asumirse el Riesgo |
| Red energética inestable | 1 | 4 | Mal funcionamiento del equipo | Alta | Reducción del riesgo, evitar, compartir o transformar |
| La ausencia de procedimiento formal para el registro y retiro de usuarios | 4 | 2 | Abusar derechos | Alta | Reducción del riesgo, evitar, compartir o transformar |
| No se tiene un proceso formal para la revisión de los derechos de acceso | 3 | 3 | Abusar derechos | Alta | Reducción del riesgo, evitar, compartir o transformar |

| | | | | | |
|---|---|---|---|---|---|
| La inexistencia de auditorias | 2 | 3 | Abusar derechos | Moderada | Asumirse el Riesgo, reducir el riesgo |
| La inexistencia identificación y valoración de riesgos | 4 | 5 | Abusos | Extrema | Reducción del riesgo, evitar, compartir o transformar |
| La inexistencia control de cambios | 4 | 4 | No cumplirse los mantenimientos de los sistemas de información | Extrema | Reducción del riesgo, evitar, compartir o transformar |
| La inexistencia de las documentaciones del MSPI | 4 | 3 | Corrupción de datos | Alta | Reducción del riesgo, evitar, compartir o transformar |
| La no existencia de políticas sobre el uso del correo electrónico | 3 | 4 | Errores | Extrema | Reducción del riesgo, evitar, compartir o transformar |
| La inexistencia de procedimiento para la manipulación de las informaciones clasificadas | 3 | 3 | Errores | Alta | Reducción del riesgo, evitar, compartir o transformar |
| La descripción de cargos no detalla la responsabilidad en seguridad de la información | 3 | 3 | Errores | Alta | Reducción del riesgo, evitar, compartir o transformar |
| La inexistencia de mecanismos de monitoreo | 2 | 3 | Robo | Moderada | Asumirse el Riesgo, reducir el riesgo |

---

*Nota.* En esta tabla se muestra el análisis de los riesgos.

**Plan de tratamiento de riesgos.** De acuerdo con el contexto, la fase de diagnóstico y las expectativas por parte de la junta directiva y los gerentes, se emite el siguiente plan para el tratamiento priorizado de los riesgos.

**Tabla 16**

*Ítems plan de tratamiento de riesgos (ISO 27002 - controles de seguridad)*

| Titulo | Descripción |
|---|---|
| Las políticas para la seguridad de la información | Desde el compromiso de la junta directiva y las gerencias, se debe precisar las políticas para la seguridad de la información, la cual debe comunicarse a las partes interesadas, garantizando su comprensión y compromiso. |
| Los roles y responsabilidades para la seguridad dela información | Precisar roles y responsabilidades en el diseño e implementación de un modelo de seguridad y privacidad de la información. |
| Términos y condiciones del empleo | Los contratos con los colaboradores y contratistas corresponden instaurar sus compromisos y las de la empresa referente a la disponibilidad, integridad y privacidad de la información. |
| Toma de conciencia, educación y formación en la seguridad | Todos los colaboradores de la organización deben de recibir sensibilización de tomar conciencia sobre las políticas y procedimientos de la organización adecuadas para su cargo. |
| Proceso disciplinario | Se debe tener unos procesos formales, administrativo e informado, para promover acciones de controles, frente a la violación de la seguridad de la información. |

| | |
|---|---|
| Finalización o intercambio de responsabilidad en el empleo | Los compromisos y obligaciones de seguridad de la información que persisten validos después de la culminación o cambio de empleo se deben especificar, comunicarlas al empleado o contratistas y que se deberían efectuar. |
| Inventariar activos | Identificación de activos con información e instalaciones de procesamiento de información, y se debe confeccionar y mantenerse los inventarios actualizados de los activos. |
| Devolución de activo | Al terminar el contrato de vinculación laboral, todos los empleados deben devolver los activos a su cargo. |
| Información debe ser clasificada | La clasificación de la información, constantemente en función de los requerimientos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. |
| Disposición de medios | Cuando ya no se soliciten los medios, disponer en forma segura, la utilización de procedimientos formales. |
| Provisión de los accesos de los usuarios | Implementar un proceso de suministro de acceso formal de los colaboradores. |
| Las gestiones de los derechos de acceso privilegiado | Implantar derechos de accesos privilegiados |
| Manipulación de información de autenticación secreta | Los colaboradores deben cumplir las prácticas de la empresa para usar autenticación secreta. |

| | |
|---|---|
| Gestiones de contraseñas | Garantizar que sean interactivos y certificar la calidad de las contraseñas. |
| Uso de aplicaciones utilitarias con privilegios | Restricción y control del uso de aplicaciones utilitarias que podrían dañar el sistema y aplicaciones. |
| Seguridad física del perímetro | Especificar y usar perímetros de seguridad, y usarlos para salvaguardar lugares que podrían contener datos confidenciales y críticos, e instalaciones de manejo de información. |
| Seguridad de las amenazas externas y ambientales | Diseño y empleo de protecciones físicas contra catástrofes naturales, irrupciones maliciosos o accidentales. |
| Las ubicaciones y protecciones de los equipos | Los dispositivos deben de estar situados y resguardados para minimizar los riesgos de amenazas y peligros del entorno, y la eventualidad de acceso no autorizados. |
| Suministros | Los dispositivos se deben salvaguardar contra fallas de energía y otras perturbaciones causadas por fallas en los servicios de energía. |
| Protecciones y seguridad del cableado | Los cables eléctricos y de comunicaciones que lleva los datos u ofrece soporte a los servicios de información se debe salvaguardar contra interceptaciones, daños o interferencias. |
| Los mantenimientos de dispositivos | Todos los dispositivos se deben almacenar adecuadamente para garantizar su disponibilidad. disponer con mantenimientos preventivos o correctivos. |

| | |
|---|---|
| Retirar los activos | Los dispositivos, información y software deben contar con autorización al momento de su retiro. |
| Disposiciones seguras o reúso de equipos | Comprobar todos los elementos de equipos |
| Las gestiones de cambios | Inspeccionar las modificaciones en la empresa, en los procesos de la operación de la empresa, en sus instalaciones y sistemas de procesamiento de información que aquejan la seguridad. |
| Gestión de capacidad | Realizar permanentemente monitoreo al funcionamiento de sus recursos, hacer los cambios, y hacer de los requisitos de capacidad futuras proyecciones, para garantizar el trabajo requerido del sistema. |
| Respaldo de la información | Realizar respaldos de la información, aplicaciones e imágenes de los sistemas, y realizar pruebas habitualmente de acuerdo con las políticas de copias de respaldo decretadas. |
| Registrar los eventos | Construir, preservar y examinar permanentemente los registros acerca de actividades de los usuarios, excepciones, fallas y acontecimientos de seguridad de la información. |
| Registros de los administradores y de los operadores | Las tareas deben estar registrados y revisados regularmente |
| Instalaciones de software en sistemas operativos | Se deben realizar procedimientos para el control de instalaciones de software en sistemas operativos. |

| | |
|---|---|
| Restricciones y prohibiciones de instalaciones de software | Los usuarios deben tener y conocer las políticas para la instalación de software. |
| Servicios de red seguros | Hallar los elementos de seguridad, los niveles de servicio y los requisitos para gestionar todos los servicios de red, y agregarlos dentro de los compromisos de los servicios de red, ya sea ejecutado internamente o sean contratados con proveedores externos. |
| Procedimientos y políticas de transferencia de datos | Tener políticas, procedimientos y controles para la transferir informaciones formales que involucre todos los canales de comunicación. |
| Mensajería electrónica | La mensajería electrónica debe estar incluida en los planes de seguridad de la información. |
| Procedimientos para el control de cambio en sistemas | El cambio en los sistemas dentro del ciclo de vida debe estar contemplados en el procedimiento de control de cambios. |
| Principio en la construcción de los sistemas seguros. | El establecimiento, documentación y mantener los principios para la reconstrucción de sistemas seguros, y emplearlos en todas las actividades de implementación de sistemas de información. |
| Ambiente de desarrollo seguro | Se debe de garantizar los ambientes seguros durante el ciclo de vida y el desarrollo del sistema. |

| | |
|---|---|
| Los procedimientos y responsabilidades | Establecer las responsables y existencia de procedimientos para las gestiones de asegurar una pronta respuesta, eficaces y ordenadas a los incidentes de seguridad de la información. |
| Reportar eventos de seguridad de la información | Los acontecimientos de seguridad de la información se deben notificar por los conductos de gestión proporcionados oportunamente. |
| Reportar las debilidades de seguridad | Todos los colaboradores y personal externo, deben reportar cualquier debilidad que observen |
| Evaluar los eventos de seguridad | Las situaciones de seguridad de la información deben ser analizadas y se debe concluir si se van a catalogarse como incidentes de seguridad de información. |
| Responder incidencias de seguridad | Se debe proporcionar contestación a las incidencias de seguridad de la información de acuerdo con procedimientos existentes. |
| Planificar de la continuidad de la seguridad | Debemos expresar los requisitos para la seguridad de la información y la continuación de las gestiones de la seguridad en circunstancias adversas. |
| Disponibilidad de infraestructuras de procesamiento de información | La disponibilidad de procesos de información debe cumplirse de acuerdo a los requisitos de disponibilidad. |

| | |
|---|---|
| Identificar las legislaciones aplicables | Identificar los requerimientos reglamentarios y contractuales, el cumplimiento, documentación explicita y actualización a cada sistema de información. |
| Derechos propiedad intelectual (DPI) | Vigilar el cumplir los derechos de propiedad intelectual. |
| Protección de registros | Salvaguardar contra perdidas, destrucciones, falsificaciones, accesos no autorizados. |
| Protección y privacidad de la información de datos personales | De acuerdo al reglamento pertinente, cuando sea aplicable. |
| Cumplir las políticas y normas de seguridad | Los directivos deben de realizar periódicamente revisión para realizar los ajustes pertinentes que promuevan la seguridad |

*Nota.* En esta tabla se muestra el plan para el tratamiento priorizado de los riesgos.

## Resultados

A partir del desarrollo técnico en la consecución de los objetivos establecidos para el presente proyecto, se arrojan los siguientes resultados.

De acuerdo con los criterios de análisis de brechas de necesidades, a partir de algunos de los numerales de la NTC-ISO/IEC 27001, se identifica un desarrollo deficiente en la seguridad y privacidad de la información.

La organización a la fecha maneja información como recurso indispensable para el cumplimiento de su actividad comercial. De acuerdo con los objetivos de la organización, la seguridad y privacidad de la información constituye un proceso estratégico, en la búsqueda de resultados deseados por las partes interesadas.

Desde las gerencias, se empieza a visualizar la necesidad de diseñar un modelo para la seguridad y privacidad de la información, que se compromete con los recursos necesarios para dar cumplimiento a los requisitos de ley y que la información sea disponible, integral y confidencial.

Se logra reconocer, que hoy se cuentan con activos importantes que no estaban inventariados, etiquetados, custodiados y asignados de forma segura a un usuario. Así mismo no se tiene claridad del tipo de información que custodia cada usuario y sus funciones y responsabilidades. En el análisis de seguridad, se identifican que 6 de 15 equipos, contienen y administran información confidencial, con alta vulnerabilidad en cuanto a la disponibilidad y susceptible en integridad.

A partir de los hallazgos, de la identificación de amenazas y vulnerabilidades y de acuerdo con las expectativas y necesidades de las partes interesadas, se genera los planes de tratamiento de los riesgos.

El presente ejercicio, contribuye al inicio de un modelo para la seguridad y la privacidad de la información en la empresa International Protection.

## Conclusiones

Se logró la identificación del estado actual de la empresa International Protection, en referencia a la gestión de seguridad y privacidad de la información, mediante la realización del diagnóstico y análisis por medio de la observación, pruebas y entrevistas realizadas directamente con los empleados en sus estaciones de trabajo.

Se realizó la planificación del sistema de seguridad de la empresa satisfaciendo las necesidades de seguridad y privacidad de la información, aplicando las recomendaciones de las guías del MSPI, donde se establecieron políticas de seguridad de la información integrando los procesos y procedimientos del negocio, estableciendo las buenas prácticas frente al trato de los datos por parte de los trabajadores de la empresa, la clientela y los contratistas con acceso a estos.

Se logró determinar los riesgos y se definió las acciones para valorar el plan de tratamiento sobre ellos, haciendo reconocimiento de vulnerabilidades y amenazas presentes y promoviendo acciones para el tratamiento del riesgo, de acuerdo con el contexto, necesidades y expectativas de la empresa.

## Referencias

Academic, 2. (2015). http://advisera.com/27001academy/es/que-es-iso27001/. http://advisera.com/27001academy/es/que-es-iso-27001/

Aguirre Cardona, J. D., & Aristizábal Betancourt, C. (2013).

Bertolin, J. A. (2008). Seguridad de la Información, Redes Informática y sistemas de información. Blog especializado en sistemas de gestión de seguridad de la información (SGSI). ISO 27001:2013. Nueva estructura. En línea}. {Consultado septiembre 2009}. https://www.pmg-ssi.com/2013/11/iso-270012013-nueva-estructura/.

Cárdenas-Solano, L. J., Martínez-Ardila, H., & Becerra-Ardila, L. E. (2016). Gestión de seguridad de la información: revisión bibliográfica. El profesional de la información (EPI), 25(6), 931-948.

Cerra, M. (2010). 200: Respuestas Seguridad. Lomas de Zamora: Fox Andina Gradi S.A.

Gómez Ravelo, C. A. (2020). Diseñar un Sistema de Gestión de la Seguridad de la Información para la Empresa Qwerty SA a partir de la Norma ISO 27001.

González, J. (2011). ¿Seguridad Informática o Seguridad de la Información? Recuperado el 02 de febrero de 2016, de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html/

Heredero, C. D., López, J. J., Agius, H., Romero Romero, S. M., Medina Salgado, S., Navarro Montero, A., & Sánchez Nájera, J. J. (2006). Dirección y Gestión de los Sistemas de Información en la empresa. Pozuelo de Alarcón (Madrid): ESIC segunda edición.

http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf;jsessionid=75BA0F422DA002AC4D56DA871D477626?sequence=1

https://www.technologyreview.es/s/10035/seis-medidas-para-proteger-las-infraestructuras-criticas-de-los-hackers. información. Madrid (España). Paraninfo.

ICONTEC (2006). Tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (sgsi), norma ISO/IEC 27001. Colombia.

Menéndez, E., Díaz, G. y Castro, M. (2009), Herramientas individualizadas para la formación en Seguridad de la Información Simulador de Ataques y Sistema de Detección de Intrusiones. TICAI 2009, 4(11), 75-82

Ministerio de Tecnologías de la Información y las Comunicaciones (2021). Modelo de Seguridad y Privacidad de la Información. Colombia.

Morales, F. E. (01 de 01 de 2004). La gestión y los gestores de la información. "Bibliodocencia". vol. 4, n. 4. http://www.bibliodocencia.com/4/4_6.pdf

Nieves, A. (2017). Diseño de un sistema de gestión de la seguridad de la información (sgsi) basados en la norma iso/iec 27001:2013. [Tesis de especialización, Institución Universitaria Politécnico Grancolombiano]. https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y.

Olmos Sosa, O y Quesada Pérez, I. (2019). Propuesta de un plan estratégico de seguridad y privacidad de la información para el Departamento Administrativo de la Función Pública (DAFP). Bogotá: Universidad Externado de Colombia, 2019.

Organisation for Economic Co-operation and Development (OECD) y Ministerio de Administraciones Públicas, Secretaría General Técnica. (2004).

Rojas Valduciel, H. (2016). Seguridad de la Información, Seguridad Informática y Ciberseguridad: ¿Son sinónimos? https://infobyteabyte.wordpress.com/2016/04/20/seguridad-de-la-informacion-seguridad-informatica-y-ciberseguridad-son-sinonimos/.

Royer, J.-M. (2004). Seguridad en la Informática de empresa. Cornella de Llobregat (Barcelona): Eni.

Vega Velasco, W. (2008). Políticas y Seguridad de la Información. Fides et Ratio- Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 2(2), 63- 69. http://www.scielo.org.bo/pdf/rfer/v2n2/v2n2a08.pdf.

Vilca Mosquera, E. C. (2017). Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa GEOSURVEY de la ciudad de lima.

Villacís Espinosa, M. L. (2016). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001: 2013 para la red corporativa de la empresa Ecuatronix (Bachelor's thesis). www.repositorio.utp.edu.co.

# Anexos

Barranquilla, 07 de octubre de 2022

Señores,
**Universidad Nacional Abierta y a Distancia UNAD**

**Por la presente notificamos a ustedes que INTERNATIONAL PROTECTION avala la ejecución del proyecto PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) presentado por Darinel Senon Contreras y Jorge Dau Janne, en calidad de y como aspirantes a grado del programa de Ingeniería de Sistemas de la UNAD.**

**Declaramos conocer y aceptar los términos y condiciones previstas para la ejecución del proyecto, estando de acuerdo con la información y actividades que surge a partir del mismos.**

**Johnny Janne**
**Gerente Aministrativo y Financiero**
**jj@internationalprotection.net**
**Cel. 3187268540**