METODOLOGÍA PARA LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN Y ANÁLISIS DE RIESGOS ORIENTADA A LAS ALCALDÍAS CATEGORÍA 6 DEL DEPARTAMENTO DE BOYACÁ

GUILLERMO ARTURO OTALORA LUNA

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

TUNJA

2020

METODOLOGÍA PARA LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN Y ANÁLISIS DE RIESGOS ORIENTADA A LAS ALCALDÍAS CATEGORÍA 6 DEL DEPARTAMENTO DE BOYACÁ

GUILLERMO ARTURO OTALORA LUNA

Trabajo de grado para optar al título de Magister en Tecnologías de la Información y la Comunicación

Asesor

JOHN FERNANDO VARGAS BUITRAGO

DOCTOR EN INGENIERIA

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

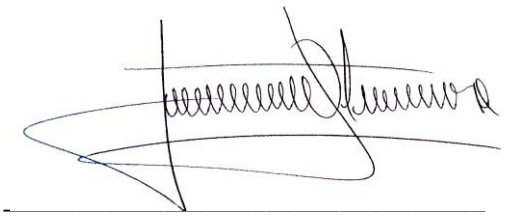
MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

TUNJA

2020

DECLARACIÓN ORIGINALIDAD

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad". Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR 

Tunja, 12 de mayo de 2020

A la memoria de… mis Padres Jorge Enrique Otálora Fajardo y Gloria Inés Luna, tíos, tías, familiares y amigos (Juan Carlos Higuera), que aunque no están conmigo en este momento, dieron todo su esfuerzo, alegría, dedicación, brindándome su cariño, apoyo y lealtad, a todos ellos dedico este triunfo en mi vida.

AGRADECIMIENTOS

A Dios por permitir latir mi corazón día a día y cumplir sueños.

A mis hermanos María Teresa, Jorge Enrique, Rosa Inés Otálora Luna, un agradecimiento especial por siempre estar apoyándome en cada decisión de la vida, por aportar sus conocimientos técnicos e investigativos en este proyecto, por su tiempo y guiarme siempre de la mejor manera.

A mis amigos de la vida, en especial a Yessid Fernando Castro Salas, por sus aportes profesionales y su alto conocimiento en el área jurídica, lo cual permitió dar un rumbo especial y significativo al proyecto de maestría.

Al ingeniero John Fernando Vargas Buitrago por siempre estar pendiente, dándome el ánimo necesario y sus valiosos aportes, observaciones y críticas frente al proyecto expuesto.

A la ingeniera Julieta Bernal, por ser esa persona que con su carisma, profesionalismo y experiencia logró darme las pautas para enfocar el proyecto de maestría.

A Dayana Bastidas por ser esa amiga incondicional, que desde la distancia me dio las fuerzas y el ánimo para llegar a la meta.

A la Universidad Pontificia Bolivariana y todo su equipo docente, administrativo y logístico, por brindarme siempre los espacios y las herramientas para llegar a feliz término con el desarrollo del proyecto.

Tabla de contenido

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

ACTIVO DE INFORMACIÓN: todos los bienes tangibles e intangibles que la organización considere importante o de alta validez en su proceso de negocio.

AUTENTICACIÓN: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico, cuando se intenta acceder a un recurso de procesamiento o sistema de información.

AUTORIZACIÓN: Consentimiento previo, expreso e informado, para el tratamiento de datos.

CLASIFICACIÓN DE INFORMACIÓN: asignar una etiqueta a un elemento según sus atributos o propiedades.

CUSTODIO DE ACTIVOS DE INFORMACIÓN: Corresponde a la dependencia o tercero que se encarga de hacer efectivas las limitaciones de acceso definidas por el responsable del activo.

MSPI: Modelo de Seguridad y Privacidad de la Información.

PROCEDIMIENTO: conjunto de acciones u operaciones que, al realizarse de la misma forma, conllevan a un mismo resultado.

PROCESO: conjunto de actividades relacionadas que al interactuar, transforman elementos de entrada en resultados o productos específicos.

RIESGO: posibilidad de que una amenaza (externa) explote una vulnerabilidad (interna) ocasionando impactos negativos en los procesos del negocio.

SGSI: un Sistema de Gestión de Seguridad de la Información es el diseño, implantación y mantenimiento de un conjunto de controles, acciones y procesos para gestionar eficientemente la confidencialidad, integridad y disponibilidad de los activos de información.

RESUMEN

Español

El presente proyecto busca proveer una metodología que pueda ser usada por las alcaldías del departamento de Boyacá que se encuentren en categoría 6, para orientar la implementación de las guías número 5 y 7 del modelo de seguridad y privacidad de la información MSPI mintic-2019-fortalecimiento-de-la-gestión-ti-en-el-estadolK,La guía número 5, gestión de clasificación de activos, está encaminada a establecer los activos posee la organización, cómo tendrían que ser usados, el rol y los compromisos que tienen los funcionarios sobre estos y la clasificación que debe dársele a cada activo de información; la guía número 7 describe la gestión de riesgo teniendo en cuenta que los activos de información son de vital importancia para la toma de decisiones, se debe proteger toda clase de Información de cualquier eventualidad de alteración, mal uso o pérdida, entre otros tipo de circunstancias que los provoquen.

Inglés

This project seeks to provide a methodology that can be used by the mayors of Boyacá department that is in category 6, to guide the implementation of guides number 5 and 7 of the ISPM information security and privacy model mintic-2019-fortalecimiento-de-la-gestión-ti-en-el-estadolK. Guide number 5, asset classification management, is aimed at determining what assets the entity possesses, how they should be used, the roles and responsibilities that officials have over them and the classification that should be given to each information asset; and guide number 7 describes risk management taking into consideration that information assets are of vital importance for decision-making, and that all types of information should be protected from any possibility of alteration, among other types of circumstances that cause.

Palabras clave

Español

Activo de Información, Gestión del Riesgo, Seguridad y Privacidad

Ingles

Information Asset, Risk Analysis, Security and Privacy.

INTRODUCCIÓN

La información a través de la historia ha sido un recurso importante, tanto así que en 1953 el gobierno nacional estableció que desde 1º de febrero de ese año el Ministerio de Correos y Telégrafos que manejaba información, a partir de ese momento se nombraría Ministerio de Comunicaciones, así mismo, años más tarde en 2009, se convirtió en Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), el cual se encargaría de liderar todo lo pertinente al tráfico de información y comunicación, esta breve evolución de la historia hace ver la importancia del por qué se debe contar con un ministerio que regule el manejo de la información y las comunicaciones en el país.

Hoy día el MINTIC se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las tecnologías de la información y las comunicaciones, por tanto, en esta era tecnológica y digital de la cual somos testigos, se considera a la información como el activo más valioso e importante en las organizaciones, de vital importancia para la toma de decisiones.

Por conflictos políticos, sociales, culturales, económicos, de imagen y demás que se presentan en los países como también dentro y fuera de las organizaciones, la información se convierte en un elemento vulnerable y está expuesta a diversos tipos de riesgos que afectan su confidencialidad, integridad y disponibilidad, entre otros factores que pueden comprometer los intereses de la organización o del estado.

Las entidades en su mayoría no están preparadas para asumir las consecuencias de la materialización de los riesgos, que en un determinado momento pudiesen atacar a los activos de información, por esta razón entre otras, el MINTIC a través de las leyes del estado Colombiano, han establecido de forma obligatoria la implementación del Modelo de Seguridad y Privacidad de la Información MSPI en las entidades gubernamentales. Teniendo en cuenta estas disposiciones se ha llevado a cabo el diseño de una metodología de levantamiento de activos de información y gestión de riesgo para aportar al MSPI el desarrollo de las guías 5 y 7 y brindar una solución a las organizaciones, esta metodología está diseñada para las alcaldías categoría 6 del departamento de Boyacá, sin embargo, el autor de este proyecto sostiene que ésta es estándar y puede ser aplicada a cualquier tipo de organización.

El informe está dividido en dos capítulos, el primero hace referencia al levantamiento de activos de información y el segundo a la gestión de riesgos, en cada uno de ellos se guía paso a paso al lector para que pueda realizar las actividades que se proponen, logrando un desarrollo completo y acertado; se establecen conceptos y definiciones importantes, se tendrán los anexos, documentos y formatos especiales que se deberán ser diligenciados en

su totalidad por quien aplique la metodología; se tendrán imágenes, cuadros explicativos, tablas con criterios de evaluación pre-establecidos para facilitar su implementación.

PLANTEAMIENTO DEL PROBLEMA

Problema

Las entidades públicas del estado colombiano dentro de todos sus procesos, generan activos de información diariamente; son de vital importancia para la toma de decisiones de la organización y su objeto misional, estos pueden estar almacenados en formatos físicos o en formatos digitales; pero sin importar su medio de conservación, a estos se les debe dar un tratamiento especial, salvaguardando y protegiéndolos de ataques, robo, daño, alteración, y demás factores que pueden comprometer los intereses de la organización o del estado.

Una de las preocupaciones expresadas por el MinTIC, es que los activos de información de las entidades del estado son vulnerables a la pérdida de la integridad, la confidencialidad y la disponibilidad, como se puede evidenciar en el documento "Modelo de Seguridad y Privacidad de la Información", en especial en las guías 5 y 7 (MinTIC, Fortalecimiento de la Gestión TI en el Estado, 2019), publicado en el portal del MINTC.

Las cifras más recientes suministradas a través de las estadísticas de gobierno en línea (GEL), sobre seguridad y privacidad de la Información en las alcaldías de Colombia, permiten apreciar que existe tan solo un 21.79% en el avance de la implementación de políticas sobre seguridad y privacidad de la información en el departamento Boyacá (Colombia), como se muestra en la Figura 1:

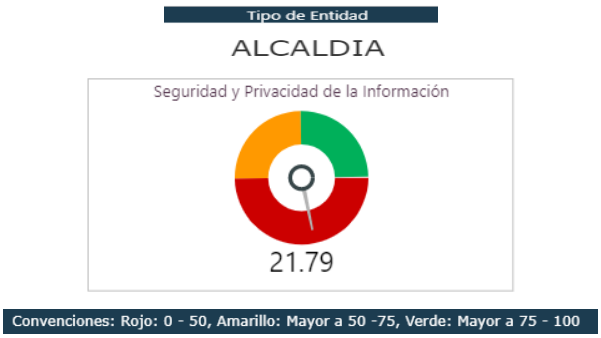


Figura 1. Implementación de políticas sobre seguridad y privacidad de la información en Boyacá

Fuente: https://colombiatic.mintic.gov.co/679/w3-propertyvalue-36675.html

Según (Furag, 2019), tomando una muestra de 116 municipios de categoría 6 del departamento de Boyacá se aprecia un promedio de 59,3% de cumplimiento en la política seguridad digital, además, según un análisis de observación realizado por el autor del

presente trabajo, con una muestra de 12 municipios en el departamento de Boyacá correspondientes al 10%, revisados los organigramas de las alcaldías de: (Chiscas, Mongua, Chíquiza, La Uvita, Aquitania, Nuevo Colón, Soata, Pachavita, Motavita, Miraflores, Ventaquemada, Socotá), se evidencia que en ninguno de ellos se cuenta con una dirección de tecnologías, sistemas de información, TIC y gobierno digital en su estructura organizacional, siendo en Boyacá, la alcaldía de Tunja en categoría 1, la única en tenerla dentro de su estructura organizacional, (Alcaldía De Tunja, 2019). Dando cumplimiento al decreto 1008 del Ministerio de las Tics de la oficina de la dirección de Gobierno Digital y al mismo tiempo al acuerdo 003 aprobado por el concejo municipal de Tunja.

Según (Manuel Santos Calderón, y otros, 2016), a 31 de diciembre de 2015:

"(i) seis de cada diez entidades públicas en el país no tiene un área de seguridad informática, ni un área de seguridad de la información; (ii) tan solo en el 21% de las entidades públicas existe un funcionario dedicado al rol de oficial de seguridad TI; (iii) en promedio, existen dos funcionarios por entidad que trabajan el tema de seguridad de la información; (iv) en las entidades públicas, los presupuestos en inversión de la seguridad son muy bajos, pues el 37% tuvo menos de 60 millones de pesos y el 24% no tuvo inversión; y (v) tan solo un 17% manifestó un aumento de presupuesto, con respecto al año anterior, dentro de la asignación del presupuesto para la inversión en seguridad. Dentro de este rubro, la inversión dirigida a protección de la red representa el 25%, y seguridad de la información el 10% (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015c)".

Ahora bien, la norma (Norma ISO 27001, 2013), considera que los activos de información son recursos del sistema de seguridad de la Información necesarios para que la entidad trascienda y se permita alcanzar los objetivos que se han propuesto desde la alta dirección, en el estudio: "Modelo de seguridad y privacidad de la información para la alcaldía de Puerto Asís en su fase de diagnóstico y planificación" (Sierra Cubides, M., & Hurtado Castrillon, 2018), se obtuvo una calificación de 1 sobre 60 en el ítem gestión de activos, para la obtención de éste valor se midieron variables con respecto al manejo de activos de información como: fallos en los sistemas informáticos, inconsistencias en la información, ausencia de soporte a funcionalidades de la organización; lo anterior permitió concluir que los funcionarios tienen un bajo conocimiento en lo que se considera un activo de información.

En cuanto a la propiedad de los activos: no se cuenta con un empalme de activos de información, se carece de asignación de roles de propietario y custodio, se desconocen los responsables y responsabilidades para que los activos estén protegidos, se carece de un manual de uso por parte de los responsables, se ignora la parte legal de sus activos de información, como lo corrobora (González Hernández, 2014), al afirmar que el 40% de las entidades no revisa la normatividad sobre seguridad de la información y el 81% nunca ha implementado un sistema de gestión de riesgos.

En las entidades del estado Colombiano, existen falencias en la clasificación de la Información, desconocimiento de los formatos en que se encuentran los activos de información y su nivel de importancia o criticidad, carencia de una clasificación según su uso, si es reservada, clasificada o pública, no se cuenta con códigos de identificación ni validación, ocasionando fallas y vulnerabilidades en los activos, como menciona (Mayorga Delgado, 2014) obteniendo riesgos como: accesos abusivos a un sistema informático, violación de datos personales, transferencia no consentida de activos entre otros delitos informáticos.

Como menciona (Alexander, 2010), en su informe: análisis del riesgo y el sistema de gestión de seguridad de la información el enfoque: ISO-27001-2005, “El propósito de la seguridad de información es asegurar la continuidad del negocio y minimizar daños a la firma previniendo y minimizando el impacto de incidentes de seguridad.”

JUSTIFICACIÓN

El diseño de una metodología para levantamiento de activos de información y análisis de riesgo, propuesto en este proyecto, busca facilitar a entidades del estado Colombiano, el desarrollo del modelo de seguridad y privacidad de la información (MSPI), brindando las herramientas necesarias para su implementación y ajustándose a los lineamientos definidos en la política pública de seguridad digital aprobada por el consejo nacional de política económica y social en el documento (Manuel Santos Calderón, y otros, 2016), que busca poner al país en alerta y reaccionar oportunamente ante riesgos de actividad maliciosa en el entorno digital.

En sin número de investigaciones el tema de la seguridad informática se considera como una disciplina de conocimiento que busca disminuir la brecha de los incidentes no esperados que puedan vulnerar los activos de una organización, y así diseñar estrategias para avanzar ante cualquier eventualidad. (Cano, Inseguridad informática: Un concepto dual en seguridad informática, 2004).

La metodología para levantamiento de activos de información y análisis de riesgo que se propone en este proyecto es apropiada y beneficia a las entidades que aún no han adoptado el modelo de seguridad y privacidad de la información, estos beneficios se verán reflejados en la protección de la confidencialidad, integridad, disponibilidad de los activos de información, cumplimiento los lineamientos del gobierno, detectando posibles amenazas y riesgos; además de formular estrategias para la toma de decisiones en la organización.

Al contar con la metodología propuesta en el presente trabajo, las alcaldías categoría 6 del departamento de Boyacá tendrán facilidades para la implementación de las guías 5 y 7 del modelo de seguridad y privacidad de la información, permitiendo así, mejorar sus índices de cumplimiento en el ítem “seguridad digital” respecto a la media nacional y asegurando un mejor manejo de sus activos de información.

La ciudadanía también se verá beneficiada, puesto que, mediante la adopción del modelo de seguridad y privacidad de la información por parte de las de las alcaldías categoría 6 en el departamento de Boyacá, se contribuirá con el aumento de la claridad en la gestión pública, incentivando el uso de las mejores prácticas de seguridad de la información como soporte

para aplicar el concepto de seguridad digital.

La metodología descrita en este proyecto es un excelente aporte para la aplicación de los lineamientos del gobierno y MinTIC relacionados con el de desarrollo y ejecución de buenas prácticas de seguridad de la información, beneficiando a las entidades del gobierno del estado colombiano en especial a las alcaldías categoría 6 del departamento de Boyacá; ésta se desarrollará cumpliendo satisfactoriamente los objetivos planteados, bajo la normatividad y parámetros establecidos en las leyes colombianas, atendiendo las necesidades comunes en las organizaciones, dando prioridad a la protección de la integridad, confidencialidad y disponibilidad de la información y sus riesgos inminentes.

El diseño de una metodología estándar para levantamiento de activos de información y análisis de riesgos orientada a las alcaldías categoría 6 del departamento de Boyacá, permitirá que las organizaciones cuenten con un análisis de activos detallado y un plan de contingencia, que brinde procesos alternativos para salvaguardar la operatividad normal de la organización.

OBJETIVOS

Objetivo General

Diseñar una guía metodológica para el levantamiento y gestión de riesgos de los activos de información de las alcaldías categoría 6 del departamento de Boyacá, tomando como referencias las guías 5 y 7 del MinTIC, para el mejoramiento de los índices de seguridad digital de estas organizaciones.

Objetivos Específicos

1. Caracterizar las variables contenidas en las guías 5 y 7 del MSPI comunes a las alcaldías de categoría 6 del departamento de Boyacá.

2. Establecer las mejores prácticas para el manejo de las variables identificadas.

3. Diseñar procesos de mitigación de riesgos basados en las guías 5 y 7 del MSPI.

4. Construir instrumentos de recolección de información de activos de información y riesgos para cada uno de los procesos diseñados.

MARCO REFERENCIAL

Marco contextual

La información es uno de los activos más importantes al interior de las organizaciones, es posible decir que es el recurso necesario e indispensable para el desarrollo y cumplimiento de las actividades de cualquier entidad; es así, que ésta puede llegar a ser sensible o crítica y por lo tanto requiere de una evaluación previa, para determinar el nivel de protección necesario para evitar y/o mitigar las posibles situaciones de riesgo e impacto que se presentan hoy día y que se encuentran relacionadas con los posibles ataques tecnológicos donde apuntarían a la pérdida de la información, y/o al retraso en la disponibilidad de la misma, así como en la calidad, integridad o confidencialidad de toda la información que es generada en el día a día.

El actor más importante en Colombia para la regulación de las normas en tecnología y comunicación, es el ministerio de las tecnologías de la información y las comunicaciones (MinTIC), que según la (MinTIC Ley 1341, 2009), o Ley de TIC, es la entidad encargada de diseñar, promover y adoptar las políticas, programas, proyectos y planes del sector de las tecnologías de la información y las comunicaciones, en sus funciones está facilitar e incrementar el acceso de todas las personas de todas las regiones a las tecnologías de la información y las comunicaciones con las ventajas y beneficios que esto trae.

La seguridad de la información y su análisis de riesgos hace parte imprescindible de cualquier procedimiento en una organización, puesto que permitirá disminuir fallos en los sistemas de información, redes, hardware, software, activos físicos y en general los activos de información que posea la entidad, por lo anterior es necesario implementar modelos que permitan la gestión de los activos de información como los menciona (Burgos Salazar & Campos), en su artículo “Modelo para la Seguridad de la Información TIC”, donde se precisa la importancia de ejercer controles y ser consecuente con la creación y ejecución de las políticas claras, estableciendo un esquema que permita regular las actividades que se van a ejercer en la organización.

El modelo de seguridad y privacidad de la información, el cual viene direccionado desde el MinTIC, está en sintonía con las buenas prácticas de seguridad y busca aportar al aumento de la claridad en la gestión pública, incentivando el uso de las mejores prácticas de seguridad de la información como soporte para aplicar el concepto de seguridad digital.

Las alcaldías del territorio colombiano son organismos públicos del gobierno que se encargan de administrar los recursos del estado, están en la obligación de cumplir con los lineamientos, normas, leyes y decretos, que se impartan desde el gobierno; en especial la Ley 1955 de 2019, por el cual se expide el plan nacional de desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad", que en su artículo 147 establece incorporar en su plan de acción el componente de transformación digital que incluye la apropiada gestión de riesgos de seguridad digital para establecer confiabilidad en los procedimientos de las entidades públicas y generar la garantía necesaria de la protección de datos personales.

Boyacá es uno de los 32 departamentos de la república de Colombia, cuenta con 123 municipios, de los cuales 116 corresponden a categoría 6, en Colombia los municipios se clasifican en categorías 1 a 6 y categoría especial de acuerdo con su número de habitantes y a sus ingresos corrientes de libre destinación –ICLD -, como lo indica la Ley 617 de 2000 en su artículo 6.

La categoría 6 corresponde a todos aquellos distritos o municipios con población igual o inferior a diez mil (10.000) habitantes y con ingresos corrientes de libre destinación anuales no superiores a quince mil (15.000 SMLV) salarios mínimos legales mensuales.

Marco conceptual

A continuación, se especifican los conceptos que se utilizan para el desarrollo del proyecto planteado, con la intención de contextualizar al lector acerca de los términos y conceptos que le permitirán comprender de manera correcta e idónea el documento.

Seguridad de la Información

Según, (NORMA ISO 27001, 2013), la seguridad de la información hace referencia a proteger y resguardar la confidencialidad, la integridad y la disponibilidad de la información importante y crítica para la organización sin importar su medio de conservación o almacenamiento, estos pueden ser físicos o digitales.

Seguridad Informática

Con el uso de los sistemas informáticos, especialmente los computadores, se ha hecho innegable el aprovechamiento de herramientas que permitan proteger la información almacenada en ellos, en especial cuando se habla de compartirla a múltiples usuarios, éstas, están diseñadas para la protección y evitar el acceso no autorizado de usuarios maliciosos

comúnmente llamados hackers. El nombre que comúnmente se utiliza para estas es seguridad informática, así lo confirma (Stallings W. , 2004), por otro lado, según (Romero, y otros, 2018), afirma que la seguridad informática es un estado de bienestar donde no existe riesgo por la confianza que se tiene en una persona o en algo, además permite gestionar los riesgos, prevenirlos, transferirlos, mitigarlos o aceptarlos.

SGSI

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conglomerado de políticas y normas para la administración de la información. El término se denomina en inglés: Information Security Management System (ISMS). Un (SGSI) cuenta con tres elementos esenciales para lograr el aseguramiento y salvaguardar la información, estos son: confidencialidad, integridad y disponibilidad, según (Alexander, 2010), controlando, monitoreando, revisando y manteniendo la mejora continua en el negocio.

Norma ISO 27001

La norma internacional ISO 27001, se centra en otorgar las directrices para el diseño e implementación y revisión de un SGSI (Mesquida A. L., Mas, Amengual, & Cabestrero, 2010), ayudando a la organización a la protección física y digital de sus activos de información.

Beneficios de la Norma ISO 27001

Las Normas internacionales permiten estar a la vanguardia, además de estandarizar y optimizar procesos, permitiendo las mejores prácticas en el área de TI, la puesta en marcha de un sistema de gestión de seguridad de información que se basa en la norma ISO 27001 otorgará a las organizaciones que usan sistemas informáticos múltiples beneficios como: competitividad, calidad a la seguridad, reducción de riesgos, concientización y compromiso y mejora continua. (Cortés R., D. M., & Ardila, 2012).

Dominios de seguridad de la ISO 27001

El salvaguardar y brindar un apropiado aseguramiento a la información, se ha convertido en un objetivo de vital importancia dentro de las organizaciones, esto con el fin de proveer la protección de sus activos de información y encaminar a la organización al éxito y continuidad en el negocio, sin embargo, para implementar un sistema de gestión de seguridad de información basado en ISO 27001, es importante conocer sus dominios dentro de los cuales se encuentran los siguientes: políticas de seguridad, aspectos organizativos, categorización y control de activos, inspección de accesos, seguridad sujeta al personal, seguridad física y del medio, desarrollo y sostenimiento de sistemas, gestión de la comunicación y las operaciones, gestión de continuidad del negocio. (Montaño Orrego V. , 2011).

Manual de Políticas de Seguridad de la Información

Se refiere al documento físico y digital donde se consignan las directrices de seguridad de la información que se encuentran implementadas en la organización, así como la definición del rol y compromisos para las actividades.

Propietario de la Información

"Propietario" no quiere decir que los activos de información son de su propiedad, significa que son personas o entidades con la responsabilidad de vigilar y cuidar que se le dé un adecuado tratamiento a estos activos, así como verificar el control de acceso a los mismos.

Confidencialidad de la información

Se habla de confidencialidad cuando se dispone de la información, pero no se divulga a terceros no autorizados, y está ligada a diferentes tipos de acuerdos internos y entre las partes. Según (Antomás & del Barrio, 2011), respecto a confidencial, se define como "Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas."

Integridad de la información

La integridad de la información es garantizar que la misma información y la forma de procesarla no ha sido alterada.

Disponibilidad de la información

La disponibilidad hace referencia a que la información estará siempre presente al momento que se requiera por los usuarios autorizados.

Autenticación

Se refiere a la forma por la cual se permite identificar y validar qué usuarios están intentando acceder a determinado sistema. Hoy día existen múltiples mecanismos de autenticación automática de personas soportadas en señales biométricas que genera la voz, la cara, el iris, la huella dactilar, como lo menciona (Ferrer Ballestrer, 2006), en su artículo autenticación de personas a partir de la biometría de la región dígito palmar.

Marco legal

En atención a las situaciones de riesgo a las que se pueden ver expuestas las entidades territoriales, es menester que estas den cumplimiento a lo establecido por el MinTIC en lo concerniente a establecer, ejecutar y mantener un modelo de seguridad de la información orientado a lograr alcanzar y sostener una cultura y conciencia en el acceso y uso adecuado

de la información en la entidad.

El MinTIC desde el año 2014 a través del mintic-2014-decreto-2573.-(12-de-12-de-2014).lK, estableció los lineamientos generales de la estrategia de gobierno en línea; en tal sentido, en el artículo 5 se fijaron los componentes que pretenden facilitar los accesos al gobierno en línea, es así, que el MinTIC ha venido trabajando para que todas las personas puedan realizar a las diligencias y tramites más importantes para su vida, completamente en online, sin tener que moverse a la entidad, sin hacer extensas filas, y de esta forma puedan ahorrar tiempo y dinero.

El Decreto 2573 de 2014 contempla acciones y proyectos de mejoramiento para la gestión institucional e interinstitucional con el uso de medios electrónicos, que deberán implementar las entidades públicas de acuerdo a lo señalado en el manual de gobierno en línea, en el cual se plasma en el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones mintic-2015-decreto-1078.lK, el cual comprende cuatro propósitos fundamentales que apuntan a lograr que todos los ciudadanos dispongan de servicios en línea de altísima calidad, promover el empoderamiento y la colaboración de los ciudadanos con el gobierno, hallar diferentes formas para que la gestión en las entidades públicas sea óptimo gracias al buen uso de la tecnología y dar garantía a la seguridad y la privacidad de la información.

El MinTIC a través del (Decreto 1078, 2015)., estableció los componentes que deben ser desarrollados a fin de masificar la demanda de gobierno en línea, de igual modo se establecen los plazos otorgados a los entes territoriales a fin de que se dé cumplimiento a la presente normativa, así las cosas, la norma en comento establece que:

Artículo 2.2.9.1.1.2. Ámbito de aplicación. Serán sujetos obligados de las disposiciones contenidas en el presente capítulo las entidades que conforman la administración pública en los términos del artículo 39 de la (Ley 489, 1998) y los particulares que cumplen funciones administrativas.

Artículo 2.2.9.1.2.1. Componentes. Los fundamentos de la estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del gobierno en línea.

Seguridad y privacidad de la Información. Comprende las acciones transversales de los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Artículo 2.2.9.1.2.3. Responsable de coordinar la implementación de la estrategia de gobierno en línea en los sujetos obligados. El representante legal de cada sujeto obligado será el responsable de coordinar, hacer seguimiento y verificación de la implementación y desarrollo de la estrategia de gobierno en línea.

Artículo 2.2.9.1.2.4. Responsable de orientar la implementación de la estrategia de gobierno en línea. En las entidades del orden territorial y demás sujetos obligados, la instancia orientadora de la implementación de la estrategia de gobierno en línea será el consejo de gobierno o en su defecto el comité directivo o la instancia que haga sus veces.

En caso de que no existan estas instancias en el sujeto obligado, será la instancia o dependencia de mayor nivel jerárquico de la entidad.

Artículo 2.2.9.1.3.1. Medición y Monitoreo. El ministerio de tecnologías de la información y las comunicaciones, a través de la dirección de gobierno en línea y de la dirección de estándares y arquitectura de tecnologías de la información, diseñará el modelo de monitoreo que permita medir el avance en las acciones definidas en el manual de gobierno en línea que corresponda cumplir a los sujetos obligados, los cuales deberán suministrar la información que le sea requerida.

En el caso de las entidades y organismos de la rama ejecutiva del poder público del orden nacional, la información será suministrada en el formulario único de reporte de avance en la gestión (FURAG) o el que haga sus veces, de acuerdo con lo señalado en función-pública-2012-decreto-2482.-(03-de-12-de-2012).lK, o las normas que lo modifiquen o sustituyan.

Artículo 2.2.9.1.3.2. Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el manual de gobierno en línea dentro de los siguientes plazos:

a. **Sujetos obligados del Orden Nacional**

COMPONENTE/AÑO	2015	2016	2017	2018	2019	2020
TIC para servicios	90%	100%	Mantener	Mantener	Mantener	Mantener

			100%	100%	100%	100%
TIC para el gobierno abierto	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la gestión	25%	50%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y privacidad de la información	40%	60%	80%	100%	Mantener 100%	Mantener 100%

Tabla 1. Sujetos obligados del orden nacional

Fuente: adaptado de https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

Artículo 2.2.9.1.3.2. Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el manual de gobierno en línea dentro de los siguientes plazos:

b. **Sujetos obligados del orden territorial.**

A. Gobernaciones de categoría especial y primera; alcaldías de categoría especial, y demás sujetos obligados de la administración pública en el mismo nivel.

B. Gobernaciones de categoría segunda, tercera y cuarta; alcaldías de categoría primera, segunda y tercera y demás sujetos obligados de la administración pública en el mismo nivel.

C. Alcaldías de categoría cuarta, quinta y sexta, y demás sujetos obligados la administración pública en el mismo nivel.

COMPONENTE AÑO	Entidades A (%)						Entidades B (%)						Entidades C (%)					
	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020
TIC para servicios	70	90	100	mantener 100	mantener 100	mantener 100	45	70	100	mantener 100	mantener 100	mantener 100	40	55	70	100	mantener 100	mantener 100
TIC para el Gobierno abierto	80	95	100	mantener 100	mantener 100	mantener 100	65	80	100	mantener 100	mantener 100	mantener 100	65	75	85	100	mantener 100	mantener 100
TIC para la Gestión	20	45	80	100	mantener 100	mantener 100	10	30	50	65	80	100	10	30	50	65	80	100
Seguridad y Privacidad de la Información	35	50	80	100	mantener 100	mantener 100	10	30	50	65	80	100	10	30	50	65	80	100

Tabla 2. Las entidades agrupadas en A, B Y C los plazos

Fuente: adaptado de https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

En conclusión, una vez verificada las normas que establecen el modelo de seguridad y privacidad de la información (MSPI), se puede determinar la necesidad de implementar dicho modelo a partir del desarrollo del material planteado por el MinTIC, el cual se encuentra publicado en la siguiente URL https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html de tal manera, que el desarrollo del modelo de seguridad y privacidad de la información, deberá estar acorde con las buenas prácticas de seguridad sujeto a los cambios técnicos de la norma (Norma ISO 27001, 2013), legislación de la Ley de protección de datos personales, transparencia y acceso a la información pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

Estado del arte

En andrade-serrano-hernán-,-otero-dajud-emilio-ramón-2009-edición,-diario-oficial;-código-penal,-congreso-de-colombialK, se describe un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”, permitiendo acceder al grupo de países que se han preparado con herramientas más eficaces para contrarrestar las acciones delictivas del ciber crimen, en sectores claves de la sociedad como el financiero, cuyas condiciones de vulnerabilidad son las más estudiadas e investigadas por los delincuentes informáticos..

Según ochoa-arévalo-2015-gobierno-de-seguridad-de-la-información,-un-enfoque-hacia-el-cumplimiento-regulatoriolK, “La Seguridad de la Información es un asunto corporativo”., afirmación que es muy importante y aplicable a los municipios, ya que la imagen de todo un gobierno y país se verá reflejada según como se maneje su información, además, este mismo autor menciona que la población en general, piensa que la seguridad de la información, incluye únicamente los sistemas de información y tecnología relacionada; sin embargo esto

tiene un mayor alcance, por lo cual es obligatorio aplicar prácticas de gobierno y gestión de seguridad de la información.

En el artículo: “Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000”, los autores valencia-duque-orozco-alzate-2017-metodología-para-la-implementación-de-un-sistema-de-gestión-de-seguridad-de-la-información-basado-en-la-familia-de-normas-iso/iec-27000lK, afirman que el conjunto de normas de la familia ISO/IEC 27000 permite la implementación de un sistema de gestión de seguridad de la información, pero advierten sobre la complejidad de este proceso, la metodología que plantea es presentada a partir de las cuatro normas que conforman dicha familia. La metodología contempla cinco (5) fases así:

- Fase 1: Aprobación de la dirección para iniciar el proyecto uno,
- Fase 2: Definir el alcance, los límites y la política del SGSI,
- Fase 3: Análisis de los requisitos de seguridad de la información,
- Fase 4: Valoración de riesgos y planificar el tratamiento de riesgos y
- Fase 5: Diseñar el SGSI.

Por su parte salazar-campos-2009-modelo-para-seguridad-de-la-información-en-ticlK, presenta un modelo que suministra un adecuado nivel de control de riesgos en tecnologías de información y comunicación (TIC), permitiendo evitar y/o disminuir las fallas en los sistemas, redes, internet y todo el patrimonio informático (hardware, software y datos) de ataques o desastres, antes que éstos ocurran. El modelo se apoya en el análisis de los estándares y normas de la seguridad de la información y su principal aporte es facilitar la implementación y/o aplicación de la seguridad de la información para TIC en cualquier tipo de organización. El modelo, puede ser tenido en cuenta como base para establecer un “Gobierno de TI” en las organizaciones que lo utilicen.

El trabajo realizado por seclén-arana-seclén-arana-2016-factores-que-afectan-la-implementación-del-sistema-de-gestión-de-seguridad-de-la-información-en-las-entidades-públicas-peruanas-de-acuerdo-a-la-ntp-iso/iec-27001lK, permite identificar los factores que afectan la implementación del SGSI en las entidades públicas y los organiza en tres niveles:

- **Nivel Estratégico:**
    - ✓ Una política estratégica de estado en seguridad de la información
- **Nivel Operativo:** 4 pilares operacionales
    - ✓ Una gestión eficiente de la seguridad de información
    - ✓ Apoyo institucional de la alta dirección
    - ✓ Una adecuada organización del SGSI
    - ✓ Aplicación efectiva de la normatividad en seguridad de información
- **Nivel Técnico:** Compuesta de 3 partes
    - ✓ Desarrollo integral institucional de la NTP
    - ✓ Contar con un presupuesto nacional para la seguridad de la información
    - ✓ La especialización técnica de profesionales en SGSI como prioridad nacional

Concluyen que el factor más importante para tener en cuenta es impulsar desde el gobierno central, es decir, promocionar una política estratégica de estado que permita formalizar funcionalmente el cargo de oficial de seguridad de Información en la estructura orgánica de las entidades del sector público. El diseño de esta política es necesario para el establecimiento operativo sobre la que se soportará la misma, como consecuencia se deriva la necesidad de "establecer la creación de un departamento de gobierno de seguridad de la información -del más alto nivel- compuesto por un grupo de especialistas en seguridad de la información que opere como un solo grupo de trabajo nacional el cual tenga como principal función un monitoreo permanente de avance y ejecución del avance de la implementación del SGSI en todas las entidades públicas peruanas, lo que podría darse a través de la potenciación funcional y técnica de la ONGEI".

En francisco-2013-diseño-de-un-sistema-de-gestión-de-seguridad-de-la-información-mediante-la-aplicación-de-la-norma-internacional-iso/iec-27001:2013-en-la-oficina-de-sistemas-de-información-y-telecomunicaciones-de-la-universidad-de-córdobalK, se toman los controles de seguridad de la ISO/IEC 27002:2013 donde se presentan los dominios (14), objetivos de control (35) y controles de referencia (114) y se plasman en el siguiente diagrama:

Figura 2. Modelo de gestión de seguridad ISO 27002

Fuente: Controles de seguridad de la ISO/IEC 27002:2013

En huillica-monzón-2015-pontificia-universidad-católicalK se especifica el concepto de HIS (Healthcare Informatics Security) como todos aquellos controles que se hayan definido en las operaciones de la entidad prestadora de salud para asegurar la seguridad de sus sistemas de información – de manera similar a un SGSI. El HIS de cualquier entidad de este tipo debe tener los siguientes objetivos:

1. Proteger la información personal.

2. Prevenir errores en la práctica de los servicios de salud.

3. Mantener las funciones de los órganos prestadores de salud (continuidad de los servicios de salud).

Para poder conseguir estos objetivos, se efectúa un análisis de vulnerabilidades, amenazas y riesgos del HIS, en el que se establecen los activos de información que deban ser protegidos contra éstos, se presentan cuatro alternativas para la administración del riesgo en este caso:

1. Establecer controles para los riesgos identificados.

2. Realizar una transferencia del riesgo hacia otra compañía, como ejemplo a través de contratos que tercericen la gestión de riesgos.

3. Aceptar el riesgo latente sin necesidad de aplicar controles para evitar su materialización.

4. Tomar medidas que busquen evitar el riesgo en los casos en los que no se haya podido establecer medidas de control apropiadas.

En nieves-2017-diseño-de-un-sistema-de-gestión-de-la-seguridad-de-la-información-(sgsi)-basados-en-la-norma-iso/iec-27001:2013lK se plantea un plan de capacitación de seguridad de la información, el cual se debe llevar a cabo de forma presencial, en un salón de actividades a través de ayudas visuales y con presencia de un experto en seguridad de la información.

Las actividades propuestas en este trabajo son:

1. Sensibilizar sobre las responsabilidades de los activos de la información a funcionarios, contratistas y personal de apoyo.
2. Concientizar a funcionarios, contratistas y personal de apoyo de la entidad de la importancia de la seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad.
3. Sensibilización de los controles de seguridad y la relación que tienen con los activos (Hardware - Software) de la información que manejan.
4. Folletos

Según stevanovi-2011-maturity-models-in-information-securitylK ISM3 es un enfoque orientado a procesos, como ITIL, según esta norma, las actividades de gestión deben seguir diferentes categorías del proceso, así:

1. **Evaluación de riesgos:** descubrir las amenazas, ataques, vulnerabilidades, para tener la imagen completa de la seguridad del sistema y determinar las prioridades de protección, en cada momento.
2. **Vigilancia**: comparación de la corriente condición del SGSI con lo proyectado, sistema documentado debe hacerse en cada momento.

3. **Ajuste**: la vigilancia es interna personaje, pero la comparación debe llevarse fuera en relación con algunos definidos externamente sistemas.
4. **Pruebas**: pruebas constantes de si las entradas del sistema dan salidas satisfactorias
5. **Mejora**: es complementario con las pruebas; seguir los resultados y buscar las posibilidades para su mejora
6. **Optimización**: un esfuerzo para reducir la entrada recursos, con la misma calidad y cantidad de las salidas

Según (Cano & Segurinfo, 2008), Si bien están tomando fuerza las unidades especializadas en delito informático en Colombia, es necesario continuar desarrollando esfuerzos conjuntos entre la academia, el gobierno, las organizaciones y la industria, para mostrarles a los intrusos que se está preparado para enfrentarlos. La inexistencia de políticas de seguridad y la falta de tiempo, no pueden ser excusas para no avanzar en el desarrollo de un sistema de gestión de seguridad.

La inversión en seguridad es costosa, pero la materialización de inseguridad puede serlo mucho más. Los resultados sugieren que en Colombia el ISO 27000, el Cobit 4.1 y las Guías del NIST son el estándar y las buenas prácticas que están en las áreas de seguridad de la información o en los departamentos de tecnología informática. Son motivadores de la inversión en seguridad: la continuidad de negocio, el cumplimiento de regulaciones y normativas internas y externas, así como la protección de la reputación de la empresa. Así mismo, se manifiesta la necesidad de adelantar al menos un ejercicio anual de análisis de riesgos como soporte a los temas de seguridad y procesos de negocio.

METODOLOGÍA

El desarrollo de la presente investigación se realizó a través de etapas como se representa en la Figura 3, debido a que el producto de cada objetivo específico fue el insumo necesario para desarrollar el siguiente; sin embargo, cada una de las etapas contempladas para la realización del proyecto, presenta una serie de características diferenciales, por lo que se hizo necesario abordar distintos enfoques metodológicos.

Figura 3. Etapas de desarrollo del proyecto

Fuente: Elaboración propia

La etapa de caracterizar variables corresponde a la definición de un diseño transversal descriptivo, en donde se "indago la incidencia de las modalidades, categorías o niveles de una o más variables en una población", además la recolección de datos se dio en un solo momento, con el objeto de describir variables, y analizar su incidencia e interrelación en un momento dado cumpliendo con las siguientes características:

- Se investigaron y determinaron las propiedades y atributos más representativos de los objetos de estudio, en este caso, las guías 5 y 7 del MSPI respecto a las alcaldías de categoría 6 del departamento de Boyacá.

- Se seleccionaron las características fundamentales del objeto de estudio, su descripción detallada y se realiza su clasificación.

Por otra parte, las etapas de establecer mejores prácticas, diseñar procesos y construir instrumentos, corresponden a un diseño transversal que "describe relaciones entre dos o más categorías, conceptos o variables en un momento determinado, ya sea en términos correlaciónales, o en función de la relación causa-efecto":

- Se analizó la asociación entre ciertos sucesos, proporcionando indicios de la relación que podría existir entre dos o más entidades capaces de influir en la predicción de un resultado específico.

- Determinó cómo se puede comportar un concepto o variable conociendo el comportamiento de una u otras variables relacionadas.

A continuación, se describen las actividades que permitieron llevar a cabo cada una de las etapas propuestas para el desarrollo del proyecto.

- **Caracterizar las variables:**

Se planteó la caracterización de las variables que determinan las propiedades y atributos más representativos de las guías 5 y 7 del MSPI respecto a las alcaldías de categoría 6 del departamento de Boyacá, para esto se desarrollan las siguientes actividades que se pueden apreciar en la siguiente tabla.

Actividad	Tarea	Producto
Descripción, recopilación, selección y clasificación de las variables presentes en las guías 5 y 7 de MSPI.	Describir las generalidades de los procesos que abarcan las guías 5 y 7.	Recapitulación de las generalidades y conceptos que integran las guías 5 y 7.
	Seleccionar las variables	Lista de variables
Identificación, asociación y modelado de los variables seleccionadas.	Identificar y describir cada una de las propiedades y atributos de las variables de las guías 5 y 7.	Tabla de variables con sus atributos y propiedades por cada una de las guías 5 y 7 del MSPI.
	Modelar la interrelación de las variables obtenidas respecto a los requerimientos de una Alcaldía categoría 6	Modelo de interrelación de las variables identificadas en las guías 5 y 7 versus los requisitos de seguridad de la información de los municipios categoría 6.

Tabla 3. Actividades – caracterizar variables

Fuente: Elaboración propia

- **Establecer las mejores prácticas:**

A partir de la caracterización de las variables que determinan las propiedades y atributos más representativos de las guías 5 y 7del MSPI respecto a las alcaldías de categoría 6 del departamento de Boyacá, se revisaron los modelos de levantamiento de activos de información y análisis de riesgos, para esto se desarrollan las actividades que se presentan en la siguiente tabla.

Actividad	Tarea	Producto
Descripción, recopilación, selección y clasificación de normas y modelos sobre gestión de activos de información.	Describir las generalidades de normas de gestión de activos de información sus respectivos modelos y métodos.	Recapitulación de las generalidades y normas de gestión de levantamiento de activos y de su riesgo.
	Seleccionar las normas de gestión de activos de información.	Lista de normas de gestión de activos de información seleccionados.
Identificación, asociación de modelos respecto de las variables seleccionadas.	Identificar y describir cada una de las prácticas seleccionadas a partir de los modelos estudiados	Descripción de las mejores prácticas sobre gestión de activos de información
	Modelar la interrelación de las variables obtenidas con las prácticas seleccionadas	Modelo de interrelación de las variables identificadas con las prácticas seleccionadas

Tabla 4. Actividades – establecer las mejores prácticas

Fuente: Elaboración propia

- **Diseñar procesos:**

Basado en los modelos de levantamiento de activos de información y análisis de riesgos, se diseñaron los procesos adecuados para una alcaldía de categoría 6, para esto se desarrollaron las actividades que se presentan en la siguiente tabla.

Actividad	Tarea	Producto
Descripción, recopilación, selección y clasificación de procesos sobre gestión de activos de información.	Describir y definir las generalidades del proceso de gestión de activos de información sus respectivos modelos y métodos para una alcaldía categoría 6	Recapitulación de las generalidades y procesos de gestión de levantamiento de activos y de su riesgo.
	Diseñar los procesos de gestión de activos de información para una alcaldía categoría 6	Diseño de modelos de gestión de activos de información seleccionados.

Tabla 5. Actividades – diseñar procesos

Fuente: Elaboración propia

- **Construir instrumentos:**

Basado en los procesos de levantamiento de activos de información y análisis de riesgos, se diseñaron los instrumentos adecuados para una alcaldía de categoría 6, para esto se desarrollan las siguientes actividades que se pueden apreciar en la siguiente tabla.

Actividad	Tarea	Producto
Diseño de instrumentos sobre gestión de activos de información.	Diseñar instrumentos que correspondan con las prácticas de la guía 5 y 7 según correlación con variables, mejores prácticas y procesos definidos.	Metodología para implementar la guía 5 y 7 del MSPI en alcaldías categoría 6

Tabla 6. Actividades – construir instrumentos

Fuente: Elaboración propia.

DESARROLLO DE LA METODOLOGIA

Para el desarrollo de este proyecto se han seguido los lineamientos de la metodología anteriormente expuesta, integrando sus resultados de manera sistémica en las metodologías de levantamiento de activos de información y gestión del riesgo que surgen como producto para ser implementadas en las alcaldías categoría 6 del departamento de Boyacá, así mismo en cualquier otra organización que requiera su aplicación, estas metodologías se pueden apreciar en los capítulos 1 y 2.

A continuación, se presentan las actividades y productos obtenidos en el desarrollo del presente proyecto.

Las siguientes actividades permiten dar cumplimiento al Objetivo 1 de este proyecto el cual es: caracterizar las variables contenidas en las guías 5 y 7 del MSPI comunes a las alcaldías categoría 6 del departamento de Boyacá.

- **Caracterizar las variables:**

Actividad - Descripción, recopilación, selección y clasificación de las variables presentes en las guías 5 y 7 de MSPI. Tomando como referencia las guías 5 y 7 del MSPI y realizando un profundo análisis, se establecieron las generalidades de los procesos, estos proponen una guía para la gestión y clasificación de activos de información, describiendo la implementación de las mejores prácticas tomando como base los lineamientos recomendados en la Norma ISO 27005, ISO 27001, ley 1712 de 2014; por otro lado se encuentra la guía de gestión de riesgos, en ella se destaca la correcta protección de la información como eje principal para el desempeño de la política pública y su relación con el ciudadano, la realización de este proyecto recapitula conceptos importantes que se integran en las guías anteriormente mencionadas, como son glosarios, definiciones, conceptos y aclaraciones especiales.

A través del estudio de las guías, se definieron las variables que se ajustan al contexto del presente proyecto, estas variables se han listado y se han concentrado dentro una serie de matrices y formatos especiales diseñados por el autor, para ser caracterizadas posteriormente según los criterios propios de cada entidad.

Los productos generados en esta actividad se pueden evidenciar en cada una de las generalidades de los capítulos 1 y 2 del desarrollo del proyecto, la lista de variables se puede apreciar en la Figura 4 y la Figura 5.

Actividad - Identificación, asociación y modelado de las variables seleccionadas: las variables fueron identificadas y clasificadas dentro de dos grandes grupos definidos como: variables dependientes e independientes, éstas a su vez, se asociaron a los procesos mencionados anteriormente y se ordenaron de tal forma que se caracterizaron acorde a los atributos propios de cada una, esta caracterización se concentra principalmente en formatos como: levantamiento de activos de información, clasificación de activos y mapa de riesgos de la información, que se describirán en el desarrollo del proyecto. Seguidamente estas variables se modelaron identificando el activo de información y sus atributos para agrupar el mayor número de características, en este caso resulta ser la ubicación del activo de información y su criticidad, lo cual hace efectivo su análisis; finalmente, se ordenaron dentro de unos contenedores genéricos definidos en el desarrollo del proyecto para pasar a la etapa de gestión del riesgo, donde se identificaron, se analizaron y se evaluaron los riesgos.

Los productos generados de esta actividad se pueden evidenciar con el diseño de la matriz de levantamiento de activos de información (Anexo 17 Matriz levantamiento activos de información), así como la matriz de riesgos de información (Anexo 18 Matriz de riesgos de la información.).

Las siguientes actividades permiten dar cumplimiento al Objetivo 2 de este proyecto el cual es: establecer las mejores prácticas para el manejo de las variables identificadas.

- **Establecer las mejores prácticas**

Actividad - Descripción, recopilación, selección y clasificación de normas y modelos sobre gestión de activos de información. La realización de este proyecto se basó principalmente en las disposiciones gubernamentales, Decreto 1078 de 2015, Ley 489 de 1998, Ley 1712 de 2014, Ley 1581 de 2012, reglamentación, Guía 5 y 7 del Modelo de Seguridad y Privacidad de la Información (MSPI), legislación de la Ley de Protección de Datos Personales, y demás normas estandarizadas como son las ISO (The International Organization for Standardization), norma técnica colombiana NTC ISO/IEC 27001, ISO/IEC 27003 e ISO 27005, COBIT e ITIL vigentes.

Los productos generados de esta actividad se pueden evidenciar con el instructivo de diligenciamiento de la matriz de levantamiento de activos y el instructivo de diligenciamiento de la matriz de riesgos de información presentes en el desarrollo de este proyecto en sus diferentes capítulos.

Actividad - Identificación, asociación de modelos respecto de las variables seleccionadas. Se extrajeron las mejores prácticas para el tratamiento de la información, éstas están presentes durante el diseño metodológico del presente proyecto, se puede resaltar el modelo de mejora continua "PDCA", (Plan, Do, Check, Act, por sus siglas en inglés), que permitirá planear, hacer, verificar y actuar; este modelo se deberá aplicar constantemente; a continuación, se nombraran las mejores prácticas de gestión de activos según la norma ISO 27001 y la ISO 27002.

Mejores prácticas según la Norma ISO 27001

- ✓ Establecer las políticas de la seguridad de la información.
- ✓ Establecer los objetivos de la seguridad de la información.
- ✓ Asegurar articulación entre los procesos de la organización y los requisitos de seguridad.
- ✓ Proporcionar los recursos necesarios para el sistema de gestión de la seguridad de la información.
- ✓ Comunicar la importancia del sistema de gestión de seguridad de la información.
- ✓ Asegurar que el sistema de gestión de seguridad de la información consigue los resultados esperados.
- ✓ Dirigir y apoyar a las personas, contribuyendo a la eficacia del sistema.
- ✓ Promover la mejora continua.
- ✓ Apoyar los procesos y roles demostrando liderazgo y compromiso.

Mejores Prácticas según la Norma ISO 27002

1. Política de Seguridad de la Información

- ✓ Organización de la Seguridad de la Información
- ✓ Gestión de activos
- ✓ Seguridad en recursos humanos
- ✓ Seguridad física y del medio ambiente

- ✓ Seguridad de las operaciones y comunicaciones
- ✓ Control de acceso
- ✓ Adquisición, desarrollo y mantenimiento de sistemas
- ✓ Gestión de incidentes de seguridad de la información
- ✓ Gestión de continuidad del negocio
- ✓ Conformidad

Las variables identificadas en el objetivo 1 se interrelacionaron en su totalidad con las mejores prácticas en mención, por tener implícito en cada una los activos de información de la entidad, a su vez se complementa al consultar en el capítulo 2 el mapa de proceso de análisis de riesgos, donde se debe tener presente el contexto estratégico organizacional.

Los productos generados de esta actividad se pueden evidenciar en cada uno de los siguientes capítulos de desarrollo del proyecto en el apartado mejores prácticas de cada capítulo.

Las siguientes actividades permiten dar cumplimiento al Objetivo 3 de este proyecto el cual es: diseñar procesos de mitigación de riesgos basados en las guías 5 y 7 del MSPI.

- **Diseñar procesos**

Actividad - Descripción, recopilación, selección y clasificación de procesos sobre gestión de activos de información. Fueron descritos y definidos los procesos de gestión de activos de información, sus respectivos modelos y métodos para una alcaldía categoría 6, basados en la guía 5 y 7 del MSPI, como se puede apreciar en el capítulo 1; el cual describe completamente la estructura del proceso de gestión de los activos de información y las actividades para el diligenciamiento de la matriz de activos, cuenta con un diagrama de procedimiento con su descripción, por otro lado en el capítulo 2 titulado gestión del riesgo, se ilustra el desarrollo del mapa de proceso de análisis de riesgos, sus generalidades y la forma de abordar un contexto organizacional orientado a la gestión del riesgo, además se destaca una evaluación previa del estado actual de la entidad a través de unas listas de chequeo que permiten complementar los procesos mencionados.

Los productos generados de esta actividad se pueden evidenciar en el diseño de esta guía metodológica, descrita a lo largo de los capítulos que la conforman.

Las siguientes actividades permiten dar cumplimiento al Objetivo 4 de este proyecto el cual es: Construir instrumentos de recolección de información de activos de información y riesgos para cada uno de los procesos diseñados.

Actividad - Diseño de instrumentos sobre gestión de activos de información. Fueron diseñados los instrumentos que se ajustaron estratégicamente con las prácticas de la guía 5 y 7 del MSPI, estableciendo correlación con variables, implementando las mejores prácticas y aplicando los procesos definidos, estas características se aprecian en el diseño de cada uno de estos instrumentos como son: listas de chequeo, matriz de levantamiento de activos, matriz clasificación de activos, matriz de riesgos, permitiendo así, en cada uno de ellos evaluar aspectos relacionados con los activos de información que posee la entidad, su seguridad y su estado actual.

Cabe resaltar que esta metodología establece los lineamientos para aplicar los instrumentos mencionados de una forma ordenada y asertiva, de forma tal, que al concluir los procesos establecidos, la entidad estará en capacidad de tomar decisiones para implementar o mejorar su sistema de gestión de la seguridad de la información.

Los productos generados de esta actividad se pueden evidenciar con los anexos entregados y con lo descrito a lo largo de los capítulos que conforman este proyecto.

PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

Este proyecto está dividido en dos capítulos, el primero hace referencia a la metodología de levantamiento de activos de información y el segundo a la metodología gestión de riesgos.

El capítulo 1 “Levantamiento de activos de información” Comienza por sensibilizar al lector acerca de la importancia de la correcta aplicación de la metodología, se muestra un resumen de los lineamientos y seguimiento, luego se presenta un listado de conceptos y definiciones importantes que se deben tener en cuenta para la comprensión del documento, enseguida se describen las generalidades que dan paso al desarrollo de esta primera parte donde se plasman los pasos a seguir como son: evaluación de la seguridad de la información de la entidad a través de listas de chequeo, la gestión de activos de información, el diligenciamiento de la matriz y la consolidación general de los activos de información, así de esta manera tener definida la primera parte de la metodología que soporta este proyecto.

El capítulo 2 “Gestión de Riesgos” inicia por consolidar generalidades que permiten concientizar al lector acerca de la importancia de protección de la información desde un contexto estratégico organizacional, enseguida se describen definiciones para la comprensión asertiva del documento, posteriormente se especifican los lineamientos que se deben tener en cuenta a nivel organizacional para ejecutar el desarrollo de la metodología, finalmente se realiza un recorrido sistémico por cada uno de los ítems del desarrollo de esta parte de la metodología, esto se resume en: analizar el contexto estratégico organizacional del sistema de seguridad y privacidad de la información, identificar los posibles riesgos, analizarlos, evaluarlos y realizar su posterior seguimiento.

El desarrollo de esta metodología está diseñado estratégicamente para alcanzar los objetivos planteados, enmarca de manera puntal y detallada cada uno de los aspectos sugeridos, permitiendo al lector visualizar su alcance e importancia al establecer una actitud de responsabilidad frente a las acciones que se deben llevar a cabo en su entidad.

A continuación, se presentarán los capítulos en mención, es indispensable seguir ordenadamente los pasos y lineamientos sugeridos en esta metodología, de esta forma su desarrollo será efectivo y no tendrá complicaciones.

CAPITULO 1

LEVANTAMIENTO DE ACTIVOS DE INFORMACION

INTRODUCCION

Esta metodología brinda los lineamientos para la identificación y clasificación de los activos de información que son manejados en la organización, donde estos se convierten en el insumo para llevar a cabo la gestión de riesgos de seguridad de la información y así mismo establecer los niveles de protección que se necesiten. El uso de esta metodología facilitará la Identificación, actualización y clasificación de los activos de información, obteniendo un insumo para la gestión de riesgos y aplicación de controles de seguridad pertinentes.

En este capítulo titulado “levantamiento de activos de información” se tendrá especial atención en el diligenciamiento de su matriz, ésta establecerá los activos de información que son de vital importancia para la entidad y a cuáles se les realizará un análisis de riesgos.

Por otro lado las variables definidas en esta metodología permitirán caracterizar los activos de información de manera tal, que se pueden identificar fácilmente para tal vez ser utilizados en algún otro tipo de proceso de tratamiento de la información.

Se ha diseñado un estratégico e innovador modelo para la clasificación de activos de información a través de contenedores, (los cuales se definirán más adelante), que permitirá organizar los activos que tengan características comunes para ser analizados de forma masiva en un solo proceso.

Las generalidades y definiciones brindadas en esta metodología, acompañadas de claros conceptos le permitirán al lector tener todo lo necesario para comprender la temática y su desarrollo, se recomienda seguir el orden de los capítulos y de cada uno de sus lineamientos para evitar vacíos e inconsistencias en su implementación.

A continuación, se listan definiciones importantes para mantener al lector en contexto con el desarrollo de la presente metodología.

DEFINICIONES

Es importante estar relacionado con los conceptos y términos que se utilizarán a lo largo de la implementación de la guía 5 del MSPI titulada Gestión de Activos de Información, por lo que a continuación, se presenta un glosario de términos que facilitarán su entendimiento.

Los términos y definiciones de gestión de activos de información se basan en la Norma NTC-ISO/IEC 27001:2013.

Alcance

Este procedimiento aplica a todos los procesos y dependencias de la organización, abarca desde la identificación y clasificación de activos hasta la propuesta de controles de riesgos.

Activo de información: Es cualquier información o elemento relacionado con el tratamiento de la misma (software, hardware, datos, edificios, personas, etc.) que tenga importancia para la organización; estos son vitales para la toma de decisiones.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, evaluación de impactos y probabilidades, para establecer las causas potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: Es el procedimiento de confirmación de la identidad de un usuario o recurso tecnológico, cuando se intenta acceder a un recurso o sistema de información.

Autorización: Consentimiento previo, expreso e informado, para el tratamiento de datos.

Confidencialidad: Es la propiedad de un documento o mensaje, que está autorizado para ser leído o entendido únicamente por las personas o entidades a las que va dirigido. Permite garantizar que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Custodio de activos de información: Corresponde a la dependencia o tercero encargado de hacer efectivas las restricciones de acceso definidas por el responsable del activo.

Disponibilidad: Es la propiedad de la información y los sistemas de tratamiento de la misma, de estar asequible y disponible cuando lo requiera una persona, entidad o proceso autorizado.

Integridad: Es la propiedad de la información relativa a su exactitud y completitud.

Propietario de activos de información: Es el dueño del activo de Información. Para la información que genera la organización, el propietario es la misma organización; para el caso en que la información sea generada por otra entidad, el propietario es dicha entidad.

Responsable de activos de información: Corresponde a la dependencia responsable de definir y revisar periódicamente las restricciones de acceso a la información y demás activos. Por lo general el responsable en la organización, es quien produce la información o se encarga de que esté disponible el activo en la entidad para el cumplimiento de sus funciones.

Usuario de activos de información: Es cualquier rol, cargo, área, entidad, sistema automatizado, servicio o equipo de laboral que genere, obtenga, transforme, conserve, elimine o utilice el activo de información físicamente o en medio digital o a través de las redes de comunicación o datos y los sistemas de información de la organización, para propósitos propios de su labor.

Normatividad y Documentos de Referencia

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Norma ISO/IEC 31000 de 2009. Gestión de Riesgos. Principios y directrices.

- Ley 1712 De 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 103 de 2015 "Por el cual se reglamente parcialmente la Ley 1712 de 2014"
- ISO/IEC 27001:2013. "Sistemas de Gestión de la Seguridad de la Información (SGSI)"
- ISO/IEC 27002:2015. Código de buenas prácticas de la gestión de la seguridad de la información.

GENERALIDADES

La guía número 5 del Modelo de Seguridad de la Información en adelante MSPI, suministrada por el Ministerio de las Tecnologías de la Información y las Comunicaciones, hace referencia a la gestión y clasificación de activos de información en las entidades de orden nacional y entidades públicas de orden territorial, además de terceros que deseen adoptar el MSPI en el marco de la estrategia de gobierno en línea.

Como parte fundamental del MSPI, la entidad a través de sus encargados de la seguridad de la información deberá realizar y poner en marcha la gestión y clasificación de activos de información que son manejados dentro de la misma, con el fin de establecer los activos que tiene la entidad, cómo deben ser caracterizados, los roles y compromisos que tienen los funcionarios sobre los mismos y el manejo según su clasificación.

El Sistemas de Gestión de la Seguridad de la Información

Un sistema de gestión de la seguridad de la información es un grupo de procesos que permitirán establecer, implementar, sostener, actualizar y mejorar continuamente la seguridad de la información al interior de la organización, tomando como raíz sus activos y los riesgos a los que están expuestos.

Su implementación claramente está dada a proteger a la organización y todo lo pertinente a sus activos de información, además de estar en concordancia con las disposiciones gubernamentales, con procesos serios y una alta definición de roles y responsabilidades, disposiciones de políticas, planes y procedimientos que deberán estar soportados y documentados.

Se establecerá un ciclo de mejora continua, atendiendo las mejores prácticas de la norma ISO 27001, se hace necesario aplicarlo y adaptarlo a las necesidades operativas y recursos de la

organización, el modelo “PDCA”, (Plan, Do, Check, Act, por sus siglas en inglés), permitirá planear, hacer, verificar y actuar, este modelo se deberá aplicar constantemente.

Planear: se planifica la implantación del sistema de gestión y seguridad de la información, se evalúa el contexto de la organización definiendo los objetivos y las políticas que permitirán alcanzarlos con el apoyo directo de la dirección.

Hacer: en esta fase se pone en funcionamiento el sistema de gestión de seguridad de la información, se entregan en práctica las políticas y controles, de acuerdo con el análisis de riesgos.

Verificar: se realiza monitoreo y chequeo del sistema de gestión de la seguridad de la información, se verifica que los procesos se realicen de la manera prevista y que se estén alcanzando los objetivos.

Actuar: permite ejecutar acciones para corregir y rectificar los fallos detectados en la anterior fase.

Contexto de la Organización

La organización que va a implementar su sistema de gestión de seguridad de la información, previamente debe entender su contexto para alinearse con sus objetivos, es fundamental conocer la organización y sus objetivos, así como todas aquellas cuestiones internas y externas que en algún momento puedan llegar a favorecer o perjudicar los procesos y procedimientos que impidan lograr estos objetivos, se debe definir el alcance del sistema de gestión de seguridad de la información, esto hace referencia a tener en cuenta los recursos de los que se dispone, la practicidad de llevarlo a los procesos y servicios más importantes de la organización, y en los posteriores ciclos de mejora ir cubriendo los faltantes.

Es de suma importancia contar con empoderamiento y responsabilidad por parte de la dirección, esto implica entre otras cosas aportar recursos económicos y humanos además de gestiones y buenas prácticas como:

a. **Establecer las políticas de la seguridad de la información:** Son los lineamientos establecidos desde la alta dirección y desarrollado por los profesionales de seguridad de la información que permitirán preservar la información y los sistemas de la organización.

c. **Establecer los objetivos de la seguridad de la información:** Se encargan de mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información.

d. **Asegurar articulación entre los procesos de la organización y los requisitos de seguridad:** Realizar reuniones con directivos y funcionarios donde se adquieran compromisos para acatar las políticas de seguridad de la información.

e. **Proporcionar los recursos necesarios para el sistema de gestión de la seguridad de la información:** La alta dirección debe destinar un rubro y así proporcionar los elementos y recursos necesarios para el sistema de la seguridad de la información.

f. **Comunicar la importancia del sistema de gestión de seguridad de la información:** Divulgar, sensibilizar, capacitar, poner en conocimiento de todos los miembros de la organización la importancia de la implementación del sistema de gestión de seguridad de la información.

g. **Asegurar que el sistema de gestión de seguridad de la información consigue los resultados esperados:** Tener presente el modelo "PDCA", el cual permitirá planear, hacer, verificar y actuar; este se deberá aplicar constantemente en el tiempo, evaluando seguidamente los resultados.

h. **Dirigir y apoyar a las personas, contribuyendo a la eficacia del sistema:** Hace referencia a brindar un soporte constante a directivos y funcionarios acerca del sistema de gestión de la información.

i. **Promover la mejora continua:** Estar implementando y renovando según normas y disposiciones gubernamentales para mantener actualizado el sistema de gestión de la información.

j. **Apoyar los procesos y roles demostrando liderazgo y compromiso:** Desde la alta dirección se deben apoyar los procesos y directrices demostrando el liderazgo, compromiso e interés por implementar y mejorar constantemente el sistema de gestión de la información.

Es necesario definir la metodología de levantamiento de activos y la metodología de análisis de riesgos como eje fundamental del sistema de gestión de la seguridad de la información, para tal fin, esta metodología estándar le permitirá paso a paso al responsable o responsables de la seguridad de la información de la organización llevar a cabo la implementación de aspectos críticos y necesarios del sistema de gestión y seguridad de la información, de una forma clara y precisa, este documento metodológico guiará al lector en los pasos que debe seguir para implementar la guía 5 y 7 de Modelo de Seguridad de la Información.

Conociendo la organización

Conocer la estructura de la organización, sus objetivos, su organigrama, los procesos y procedimientos que se llevan al interior de esta, le permitirá llevar a cabo la implementación un sistema de gestión seguro y confiable, por tal razón el primer paso que el lector o el equipo de seguridad de la información o sus encargados deberá realizar, es evaluar su organización a través de 16 listas de chequeo propuestos en esta metodología.

Cada lista de chequeo mide aspectos relacionados con seguridad, protección y gestión, si se cumplen totalmente, la organización es ejemplar en gestión de la seguridad de la información, de lo contrario, esta guía metodológica llevará al lector a desarrollar e implementar las guías 5 y 7 del MSPI de una forma práctica y organizada, dando los primeros pasos en la implementación de un sistema de gestión de seguridad de la información.

DESARROLLO

PASO 1 - EVALUACIÓN A TRAVÉS DE LISTAS DE CHEQUEO

Se establecerá la situación real y actual de la organización, para esto el encargado o encargados de la seguridad de la información, deberán diligenciar las 16 listas de chequeo que estarán disponibles en los Anexos del 1 al 16., estas listas de chequeo fueron diseñadas por el autor de este proyecto basadas en la experiencia y otros documentos de referencia.

En cada una de estas listas de chequeo se encontrarán los aspectos a evaluar, estos medirán las condiciones en las cuales la organización se encuentra actualmente, el análisis de esta información permitirá tomar las acciones respectivas en la implementación o mejora del sistema de gestión de la seguridad de la información.

Estas listas de chequeo están estructuradas de tal forma que en la primera parte se evalúa si el aspecto existe o no en la organización, de existir, establece un valor en porcentaje que indica el avance de este ítem.

Los siguientes serán los aspectos generales para evaluar:

1. **Seguridad de la información:** Su objetivo es proporcionar dirección gerencial y apoyo a la seguridad de la información alineado con los requerimientos organizacionales y leyes vigentes.
2. **Gestión de activos:** Su objetivo es alcanzar y conservar la protección apropiada de los activos organizacionales.

3. Seguridad de los recursos humanos: Su objetivo es asegurar que los empleados, comprendan sus responsabilidades y estos sean apropiados para los roles que se les considera; disminuir el riesgo de robo, fraude o mal uso de los medios.

4. Seguridad física y ambiental: Su objetivo es evitar el acceso físico no autorizado, daño e interferencia al área de sistemas y la información de la organización.

5. Seguridad en la infraestructura: Su objetivo es confirmar el conocimiento que se tiene en la infraestructura del centro de datos y los sistemas de control establecidos.

6. Seguridad de equipos: Su objetivo es impedir la pérdida, daño, robo o exposición de los activos y la interrupción de las actividades de la organización.

7. Gestión de las comunicaciones y operaciones: Su objetivo es garantizar la operación correcta y segura de los medios de procesamiento de la información.

8. Planeación y aceptación del sistema: Su objetivo es disminuir el riesgo de fallas en los sistemas.

9. Protección contra software malicioso: Su objetivo es salvaguardar la integridad del software y la información de la organización.

10. Gestión de seguridad de redes: Su objetivo es garantizar la protección de la información de redes y la protección de la infraestructura de soporte.

11. Intercambio de información: Su objetivo es conservar la seguridad de la información y software intercambiados dentro de la organización y con cualquier entidad externa.

12. Monitoreo: Su objetivo es detectar actividades de procesamiento de información no autorizada.

13. Control de acceso: Su objetivo es Controlar acceso a la información.

14. Responsabilidades del usuario: Su Objetivo es evitar el acceso de usuarios no autorizados y el compromiso o robo de la información y los medios de procesamiento de la información.

15. Control de acceso a redes: Su objetivo es evitar el acceso no autorizado a los servicios de red.

16. Seguridad en los procesos de desarrollo y soporte: Su objetivo es mantener la seguridad del software e información del sistema de aplicación.

Forma de evaluar las listas de chequeo

Una vez se han aplicado las listas de chequeo en la entidad, se debe calcular el promedio de valores por cada ítem mencionado anteriormente y así se tendrá una estimación en

porcentaje y se conocerá el estado actual de la organización comparándolo con la siguiente tabla.

Rangos de Porcentaje %	Estado del ítem evaluado
0% &< 10%	Deficiente
10% & <30%	Malo
30% & <70%	Regular
70% & < 80 %	Bueno
80% & < 90 %	Excelente
90% & < 100 %	Sobresaliente

Tabla 7. Valores para evaluar ítem de seguridad

Fuente: Elaboración propia

PASO 2 - GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN Y DILIGENCIAMIENTO DE MATRIZ

El sistema de gestión de la seguridad de la información, permitirá mejorar la seguridad de los procesos, procedimientos y servicios llevados en la organización que estén incluidos en el alcance, cuyo funcionamiento depende del conjunto de activos de información: información física, información digital, aplicaciones, servidores, equipos de cómputo, comunicaciones, personas, entre otros.

Definición de variables: Se definen como variables independientes "identificación básica del activo" como se observa en la Figura 4 y como variables dependientes "criticidad del activo" como se aprecia en la Figura 5.

IDENTIFICACION BASICA DEL ACTIVO
Código Identificación del Activo
Nombre del Activo de Información
Proceso
Procedimiento
Descripción
Propietario
Responsable
Custodio
Usuarios
Tipo de Información
Medio de Conservación
Formato
Idioma
Ubicación
Respaldo
Clasificación según SIG
Publicación
Observación
Soporte Legal

Figura 4. Variables independientes

Fuente: Elaboración propia

CRITICIDAD DEL ACTIVO
Clasificación según Disponibilidad
Clasificación según Confidencialidad
Clasificación según Integridad

Figura 5. Variables Dependientes

Fuente: Elaboración propia

Teniendo en cuenta lo anterior, es importante conocer y registrar los activos de información propios de la entidad, a continuación, una breve definición:

Activo de Información:

De acuerdo con el glosario de términos de la norma ISO/IEC 27000, define a un activo de información como cualquier información o componente relacionado con el tratamiento de la misma (software, hardware, documentos físicos, datos, aplicativos, personas) que tenga valor para la organización.

Una vez el lector conoce el objetivo y la importancia de registrar los activos de información para salvaguardar su confidencialidad, integridad y disponibilidad, seguirá esta metodología de levantamiento de activos, adaptándola al contexto de su entidad protegiéndola de posibles riesgos.

Diligenciamiento Matriz de Activos de Información

Para esta metodología se ha creado una matriz de levantamiento de activos de información que se encuentra en el Anexo_17_Matriz Levantamiento Activos De Información, el encargado o los encargados de la seguridad de la información de la organización, deberán diligenciarla en su totalidad, llevándola a cada una de las dependencias y por cada uno de los funcionarios pertenecientes a la entidad, el objetivo principal es realizar un inventario de cada uno de los activos que posee la entidad, además de una evaluación del grado de su criticidad (critico, alto, medio o bajo), en las siguientes figuras se presenta la matriz de activos de información por partes.

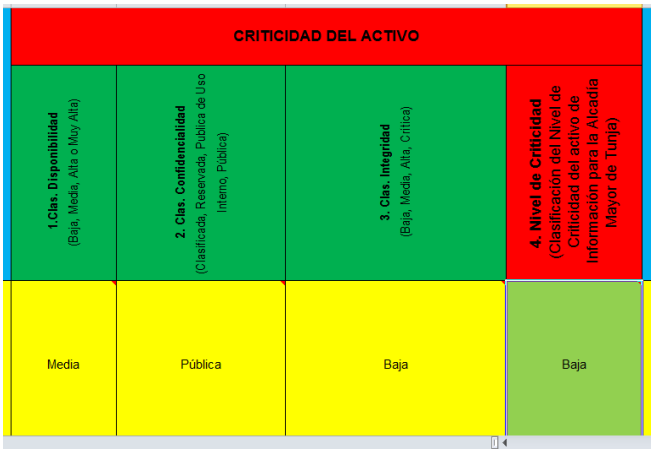
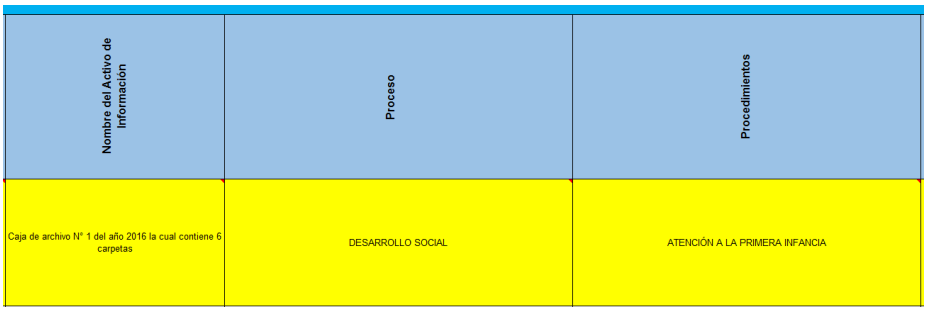


Figura 6. Matriz levantamiento de activos (parte a)

Fuente: Elaboración propia



Nombre del Activo de Información	Proceso	Procedimientos
Caja de archivo N° 1 del año 2016 la cual contiene 6 carpetas	DESARROLLO SOCIAL	ATENCIÓN A LA PRIMERA INFANCIA

Figura 7. Matriz levantamiento de activos (parte b)

Fuente: Elaboración propia

Idioma	Ubicación del Activo de Información (Física o Digital)	Respaldo (SI/NO/NA)
Castellano	SECRETARIA DE LA MUJER EQUIDAD DE GÉNERO Y DESAROLLLO SOCIAL CAJA N° 1 OFICINA NUTRICIÓN, SOBRE EL ARCHIVADOR	NO

Figura 8. Matriz levantamiento de activos (parte c)

Fuente: Elaboración propia

Instructivo Diligenciamiento de la Matriz de Activos de Información

En la Matriz de Activos de Información se encuentran las siguientes casillas para diligenciar, algunas tendrán texto libre y otras serán exclusivamente de selección.

En seguida, se presentan las instrucciones de diligenciamiento de la matriz de activos de información.

- **Encabezado:**

Nombre del Dominio: Nombre del dominio hace referencia al valor estático al cual pertenece la matriz, en este caso será: “Clasificación de la Información y Activos de Información”

Nombre del responsable del Inventario: Nombre del funcionario responsable de levantar el inventario de activos de Información de cada dependencia.

Dependencia: Es el área, dependencia o secretaría en la cual se realiza el inventario de activos de Información.

Fecha de elaboración: Fecha en la cual se inicia el levantamiento del inventario de activos de Información.

- **Contenido de la Matriz**

Código de identificación del activo: Identifica el activo de información de acuerdo con la siguiente estructura: **XXX-YYY**, donde XXX identifica el área de la Organización y YYY un consecutivo numérico para identificar el activo de información del área o dependencia.

Nombre del activo de información: Corresponde al nombre con el cual se identifica el activo dentro del área a la cual pertenece, este debe ser significativo y relacionado con la información que contiene.

Proceso: Identifica el Proceso al que pertenece el activo de información. Corresponde a los formalizados en la organización.

Procedimientos: Identifica el Procedimiento que depende del Proceso seleccionado en la Organización.

Descripción: Es un área para describir el activo de manera única, clara y de fácil identificación por todos los miembros del proceso. Se debe relacionar información adicional que le brinde importancia al activo dentro de la entidad y su proceso.

Propietario: Es el dueño del activo de Información. Para la información que genera la organización, el propietario es la misma organización; para el caso en que la información sea generada por otra entidad, el propietario es dicha entidad.

Responsable: Corresponde a la dependencia garante de definir y revisar periódicamente las restricciones de acceso a la información y demás activos. Por lo general el responsable en la organización, es quien produce la información o se encarga de que esté disponible el activo en la entidad para el cumplimiento de sus funciones.

Custodio: Corresponde a la dependencia o tercero delegado para hacer efectivas las limitaciones de acceso definidas por el responsable del activo.

Usuario: Es cualquier rol, cargo, área, entidad, sistema sistematizado, servicio o equipo de trabajo que genere, transforme, obtenga, conserve, elimine o utilice el activo de información físicamente o en medio digital o a través de las redes y los sistemas de información de la organización, para designios propios de su labor.

Tipos de activo de información: Son los principales grupos o categorías en los que se clasifican los activos de información y pueden ser de cinco tipos:

1. **Información:** Son datos digitales o físicos, en cualquier formato que se genera, almacena, gestiona, transmite y destruye en la entidad. Por ejemplo: Bases de datos, contratos, manuales de usuario, procedimientos, informes de auditoría, código desarrollo, documentos relativos a las investigaciones, procedimientos, guías, protocolos, archivos de audio, carpetas contenedoras de información, expedientes físicos, documentos del archivo físico de gestión, entre otros.

2. **Software:** Aplicaciones Informáticas que se utilizan para la gestión de la información. Por ejemplo: Software de Aplicación, sistemas operativos, herramienta de desarrollo, motor de bases de datos, controladores de dispositivos, herramientas ofimáticas, antivirus, software de diseño y programación, compiladores, entre otros. Se recomienda que este tipo de activo de información lo registre solo la dependencia responsable o encargada de que este tipo de activo esté disponible en la Entidad, es decir la dependencia que lo contrata o crea.

3. **Hardware:** Equipos de comunicaciones, computadores, portátiles, tabletas, teléfonos inteligentes, que por su criticidad son considerados activos de información, no sólo activos fijos. Son todos aquellos que soportan el procesamiento de información y la funcionalidad de los servicios de red. Por ejemplo: Computador de escritorio, Computador portátil, Switches, Hubs, Firewall, Tablet, Teléfono inteligente etc. Se recomienda que cada dependencia diligencie los activos de hardware correspondientes a los equipos de cómputo y/o dispositivos móviles dados por la Entidad para el cumplimiento de sus funciones, y los activos que soportan la información como los servidores, discos externos etc., o dispositivos de comunicaciones sean identificados por la dependencia que los adquiere o contrata.

4. **Infraestructura Física:** Es la infraestructura física que soporta el funcionamiento de la entidad. Por ejemplo: Edificio principal de la Organización, Área de almacenamiento de archivo de gestión físico, Archivadores que contienen carpetas físicas, Centro de procesamiento de datos (Data Center), etc. Se recomienda que cada dependencia encargada de suministrar la disponibilidad del sitio, espacio o zona, sea quien registre este tipo de activo, por ejemplo: Archivador que contiene información personal en formato físico de los funcionarios y contratistas de la organización lo debe identificar el usuario de la dependencia de Talento Humano. Todo lo anterior con el fin de que no se presenten duplicidades en la identificación de los activos.

5. **Redes:** Corresponde a los servicios comunicaciones compartidas, tales como Internet, páginas de consulta, directorios compartidos, Intranet, etc. Se recomienda que estos activos los identifique la dependencia que los contrata o pone a disposición para el funcionamiento en la Entidad.

6. **Servicios Tercerizados:** Corresponde a las funciones realizadas por empresas o Entidades externas que son expertas en el campo contratado. Se recomienda que estos activos de información los registre la dependencia que los contrata.

7.**Personas:** Aquellas personas (recurso humano) que, por su experiencia y sabiduría en los procesos, son consideradas como activos de información, y que dichas actividades no están relacionadas en los procedimientos o documentos formales de la Entidad, y por tanto si esta persona no está disponible para ejecutar las actividades, podría generarse un impacto negativo en el proceso.

Medio de conservación del activo de Información: Indica si el activo se encuentra en medio físico (F) o digital (D).

Formato: identifica el tamaño, forma, y la manera en la que se presenta la información o se permite su visualización o consulta. Se debe seleccionar una de las siguientes opciones:

Texto (incluye extensiones como .doc, .txt, .rtf, .pdf)

Hoja de cálculo (incluye extensiones como .xls, .xlt, .csv)

Presentación (incluye extensiones como .ppt, .pps)

Documento gráfico (incluye extensiones como .jpg, .gif, .png, .tif, .tiff, .ttf)

Base de datos (incluye extensiones como .mdb, .sql)

Audio (incluye extensiones como .wav, .mid, .mp3, .ogg)

Video (incluye extensiones como .mpeg, .avi, .mov .mp4)

Animación (incluye extensiones como .swf)

Compresión (incluye extensiones como .zip, .rar)

Código fuente (incluye extensiones como .html, .htmls, .php,.jar,)

Impreso (Papel)

Correo electrónico

Mensajería instantánea

Varios (incluye varios tipos de formatos)

N/A: seleccionar cuando los activos de información son software, hardware, personas o servicios tercerizados.

Idioma: Indicar el idioma, dialecto o lenguaje en el que se encuentra la información. Se debe tener en cuenta que el idioma oficial de Colombia es el castellano y otras lenguas y dialectos de grupos étnicos son también oficiales en sus territorios. Hoy existen en Colombia 65 lenguas indígenas y 2 lenguas criollas se puede verificar esa información en el siguiente enlace https://www.radionacional.co/noticia/cultura/10-datos-sobre-las-lenguas-nativas-de-nuestro-pais

Ubicación del activo:

Física: Especifica la ubicación de los activos de información en formato físico (Edificio, piso, costado, área, oficina, centro de cómputo, bodega, archivador, carpeta y sector) bajo el cuidado del custodio de la información.

Digital: Especifica el lugar de los activos de información de forma digital, que están bajo el cuidado del custodio de la información, tales como: servidores, computadores , medios de almacenamiento externos e internos , carpeta digital privada o pública, bases de datos, sistema de información, nombre del servidor (base de datos, aplicaciones) o url.

Respaldo (SI/NO/NA): En este campo se debe diligenciar SI, si el activo de información requiere copia de respaldo, que podría ser restaurada en caso de requerirse. Indicar NO, si la información no requiere respaldo. Indicar NA en el caso que no aplique para el tipo de activo de información en cuestión. El respaldo de dicho activo puede a su vez ser considerado un activo de información. Es decir que se puede registrar la Copia de respaldo de XXXX información como un activo.

Preguntas de Orientación: Se generaron 8 preguntas de orientación para tener en cuenta en la valoración de los criterios de seguridad de la información.

1. La información contiene datos personales (LEY 1581)

2. La información es de cumplimiento Legal? Indique número de Ley, Decreto, CONPES, etc. En el campo de observaciones

3. ¿La información requiere de algún tipo de control que le brinde protección especial? Ejemplo. Cifrado, envío con clave, datos enmascarados

4. ¿El Activo necesita de permisos especiales para acceder?

5. ¿La información del activo es exclusivamente de uso interno?

6. ¿En caso de pérdida de esta información, se incurriría en algún tipo de pérdida económica, multa, sanción o daño?

7. ¿La información es para uso exclusivo del propietario o responsable?

8. ¿Si la información no está disponible rápidamente por algún suceso inesperado, afecta críticamente el desarrollo del proceso?

Clasificación de la Información:

La clasificación de activos de información tiene como propósito, garantizar que la información establece las capas de protección adecuadas y que por sus características necesita un tratamiento especial. El sistema donde se clasifica la información que podría precisar en la entidad, está basado en las características propias de la información; tiene en cuenta el funcionamiento interno de la entidad, siempre procurando dar cumplimiento a los lineamientos y requisitos estipulados en el ítem relacionado con la Gestión de Activos de los estándares ISO 27001:2013, ISO 27002, e ISO 27005. La norma ISO 27001 no establece unos niveles de clasificación en concreto, sino que cada entidad, bajo sus criterios y características propias, debe definir sus argumentos de clasificación concretos.

Una organización establecerá más niveles de clasificación a medida que la misma sea de mayor tamaño y presente una mayor complejidad, para esta metodología se clasificaran los activos de información según criterios de su disponibilidad, confidencialidad e integridad.

Cada uno de los criterios de clasificación de activos tiene diferentes niveles con valoraciones numéricas establecidas por esta metodología del 1 al 4, esto con el fin de cuantificar la criticidad del activo de información, se pueden apreciar en la Tabla 8, la Tabla 9 y la Tabla 10.

La función REDONDEAR, aproxima un valor numérico en decimales a un número entero.

La ecuación utilizada es: REDONDEAR ((Valor Nivel Seleccionado en Disponibilidad + Valor Nivel Seleccionado en Confidencialidad + Valor Nivel Seleccionado en Integridad)/3)

Los Colores juegan un papel muy importante, con ellos se puede identificar rápidamente de forma visual la criticidad del activo para su clasificación y tratamiento.

	Nivel	Valor
Disponibilidad	Baja	1
	Media	2
	Alta	3
	Muy Alta	4

Tabla 8. Valores para evaluar disponibilidad

Fuente: Elaboración propia

	Nivel	Valor
Confidencialidad	Información pública	1
	Información pública de uso interno	2
	Información pública clasificada	3
	Información pública reservada	4

Tabla 9. Valores para evaluar confidencialidad

Fuente: Elaboración propia

	Nivel	Valor
Integridad	Baja	1
	Media	2
	Alta	3
	Crítica	4

Tabla 10. Valores para evaluar integridad

Fuente: Elaboración propia

Clasificación de acuerdo con la disponibilidad: Consecuencia que se genera para la entidad cuando el activo de información no consigue estar disponible cuando se necesita.

Baja (1): Información donde la imposibilidad de acceso no afecta en forma significativa el movimiento de la entidad y puede no estar disponible más de una semana.

Indisponibilidad: mas + de una semana (1 semana = 7 días calendario)

Media (2): Información donde la imposibilidad de acceso por un periodo de entre 3 y 7 días puede ocasionar pérdidas o sanciones la entidad.

Indisponibilidad: entre 3 y 7 días calendario.

Alta (3): Información donde la imposibilidad de acceso por un periodo de 1 a 3 días ocasiona pérdidas mayores y/o sanciones a la entidad.

Indisponibilidad: entre 1 y 3 días calendario.

Muy Alta (4): Información donde la imposibilidad de acceso por menos de 1 día ocasiona pérdidas mayores y/o sanciones a la entidad.

Indisponibilidad: menos de 1 día calendario.

Clasificación de acuerdo a la Confidencialidad: Nivel de Acceso a la información. El activo sólo sea accedido, por personas, procesos o entidades estén autorizados.

Información pública (1): Es toda información que ha sido declarada de acceso público, de acuerdo con las normas existentes por la persona o grupo de personas de la entidad responsables del activo de información y que por lo tanto no tendrían condiciones de seguridad frente a la confidencialidad.

Información pública de uso interno (2): Es toda información que la pueden conocer y utilizar todos los funcionarios de la entidad, puede ser divulgada a algunas entidades externas debidamente autorizadas por el propietario, puede encontrarse en proceso de construcción y no requiere su divulgación a terceros, pero es necesaria para las actividades internas de la entidad, y cuya divulgación y uso no permitido podría ocasionar riesgos o pérdidas leves para la entidad. Ejemplo: Información de la Intranet, publicaciones internas, documentos en construcción etc.

Información pública clasificada (3): Como lo prescribe la Ley 1712 de 2014, información pública clasificada es aquella información que estando en poder o

custodia de un sujeto obligado en su calidad de tal, pertenece al propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014. Esta corresponde a toda aquella información que pudiere causar un daño a los siguientes derechos:

a) El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.

b) El derecho de toda persona a la vida, la salud o la seguridad.

c) Los secretos comerciales, industriales y profesionales.

También corresponden a esta categoría los datos que son catalogados como "dato semiprivado o privado" de acuerdo al decreto 1377 de 2013; además de los datos de uso interno de la entidad y que no deben ser conocidos por el público en general.

Información pública reservada (4): En los términos de la Ley 1712 de 2014, la información pública reservada es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014. Se trata de una información que solo puede ser conocida y utilizada por un grupo muy reducido de empleados debidamente autorizados por el responsable de la información, generalmente de la alta dirección, y cuya divulgación o uso no autorizados podría ocasionar pérdidas. Información relacionada con:

a) La defensa y seguridad nacional;

b) La seguridad pública;

c) Las relaciones internacionales;

d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;

e) El debido proceso y la igualdad de las partes en los procesos judiciales;

f) La administración efectiva de la justicia;

g) Los derechos de la infancia y la adolescencia;

h) La estabilidad macroeconómica y financiera del país;

i) La salud pública.

También corresponde a información de carácter reservado los datos catalogados como sensibles por el decreto 1377 de 2013.

Clasificación de acuerdo con la Integridad: Establece cuál es el efecto de la alteración no permitida de los datos del activo de información, el impacto que tendría en los procesos donde se encuentra comprendido y a su vez que efectos que podría tener para la entidad.

Baja (1): Información cuya modificación no autorizada, pérdida de exactitud y falta de datos se puede remediar. Se afecta solo un porcentaje del proceso y no hay pérdida económica. Completar

Media (2): Información cuya modificación no autorizada, pérdida de exactitud y falta de datos, podría repararse parcialmente, puede conllevar a un impacto negativo de índole legal, se afectan varios procesos generando retrasos en las actividades y los daños implican pérdidas económicas moderadas.

Alta (3): Información cuya modificación no autorizada, causa pérdida de exactitud y falta de datos, podría no repararse completamente, se afectan varios procesos misionales generando un impacto negativo de índole legal y/o pérdidas económicas, y se retrasan las funciones de la entidad.

Crítica (4): Información cuya modificación no autorizada, causa pérdida de exactitud y falta de datos, podría no repararse completamente, afecta a toda la organización generando un impacto negativo de índole legal y económico, retrasa las funciones, y los daños son casi irreparables.

Nivel de Criticidad o importancia del Activo de Información: estableciendo los niveles seleccionados en la Disponibilidad, Confidencialidad e Integridad, se obtiene el nivel de criticidad o importancia del archivo, que será el común denominador para la clasificación de los activos de información, en la matriz suministrada en esta metodología el resultado

Baja: Son aquellos que no contienen información crítica, y por lo tanto no les debe realizar identificación de riesgos ni aplicar controles de seguridad específicos, políticas, estrategias, procedimientos entre otros., que coadyuven con la mitigación y control del riesgo.

Media: Son aquellos que tienen información apoyan en pocos procedimientos del negocio, se les debe realizar identificación de riesgos y aplicar controles de seguridad políticas, estrategias, procedimientos etc., que coadyuven con la mitigación y control del riesgo.

Alta: Son aquellos que apoyan en muchas actividades del negocio, se les debe realizar identificación de riesgos y aplicar controles de seguridad específicos o especializados, políticas, estrategias, procedimientos etc., que coadyuven con el control del riesgo.

Critica: Aquellos que son muy importantes para la entidad porque aportan en el desarrollo de actividades críticas que se relacionan directamente con la misión, es decir que son críticos para la continuidad del negocio, se les debe realizar identificación de riesgos y aplicar controles.

Clasificación de la Información según sistema integrado de gestión de la entidad: Se registra aquí el nivel de clasificación dado a la información de acuerdo con la normatividad vigente. Sin embargo, se incluyen otras clasificaciones que el propietario podría utilizar:

- **Confidencial:** acceso restringido a la alta dirección.
- **Restringido:** directores de área y empleados especiales tienen acceso.
- **Interno:** accesible para algunos miembros de la organización, pero en cualquier nivel.
- **Público:** todas las personas, dentro y fuera de la organización, tienen acceso.

El activo se encuentra publicado y/o disponible:

Se debe seleccionar si la información está publicada o disponible para ser requerida por otras dependencias o por el ciudadano, indicando dónde está publicada y/o dónde se puede revisar o solicitar. En este campo debe seleccionar alguna de las siguientes opciones:

- Publicado: Escribir el sitio web de consulta
- Disponible: Escribir el repositorio interno donde se encuentra disponible
- Publicado y disponible: Escribir el sitio web, y repositorio interno de disponibilidad.
- Disponible pero no publicado: Escribir N/A
- Ni disponible ni publicado: Escribir N/A

Lugar de Consulta: Indicar la ruta(s) o lugar(es) donde está publicado o puede ser revisado el activo de información, tales como: Url en el sitio web, SharePoint u otro medio(s) en donde se puede descargar y/o acceder a la información. Solo aplica para el tipo de activo información, para el caso de los demás activos escribir N/A

Observaciones (aclaraciones/excepciones): Se incluye aquí cualquier información relevante para el proceso de clasificación de activos de información o el análisis de riesgos asociado. Se pueden incluir las aclaraciones que se consideren necesarias sobre el activo de información.

Soporte Legal: En caso de que el activo de información este soportado legalmente se debe incluir el nombre del Artículo, Resolución, Ley, Decreto, Política, entre otros.

Con este último ítem, se finaliza el diligenciamiento de la matriz de levantamiento de activos de información, de preferencia ningún campo dentro de la matriz debe quedar sin diligenciar para llevar a feliz término el desarrollo de la metodología expuesta.

El siguiente es el procedimiento de las actividades que se debe cumplir al interior de la organización para efectuar el levantamiento de la matriz de activos de información de una forma ordenada y concreta.

Procedimiento de las actividades para levantamiento de matriz de activos de información en la entidad

En la Tabla 11 se aprecia el procedimiento a seguir para realizar el levantamiento de activos de información en la entidad.

Actividad	Descripción	Responsable	Registro
1. Invitar a los enlaces o encargados de las diferentes dependencias a la Socialización de la Matriz de Inventario de Activos	Por parte de los encargados de la seguridad de la información, deberán enviar a todos los enlaces o encargados de las diferentes dependencias, una circular solicitando su presencia para socializar el diligenciamiento de la matriz de activos de información.	Encargado o encargados asignados para gestionar la seguridad de la información,	Circular
2. Socializar Matriz de Inventario de Activos con los enlaces de las Diferentes dependencias y funcionarios	Por parte de los encargados de la seguridad de la información, se realiza la presentación y socialización de la Matriz de inventario de activos a los enlaces de las diferentes dependencias	Encargado o encargados asignados para gestionar la seguridad de la información,	Listas de asistencia, Fotografías Memorias de la presentación
3. Asignar la identificación y actualización de los activos de información	Delegar a los funcionarios a través de los enlaces o encargados de las dependencias el diligenciamiento de la Matriz de inventario de activos	enlaces o encargados de las diferentes dependencias	Correo electrónico
4. Realizar el levantamiento de los activos de información	Diligenciar en su totalidad la matriz de activos de información.	Usuario/funcionarios	Matriz de activos de información diligenciada
5. Remitir la matriz de activos de información consolidada por dependencia	Remitir la matriz de activos de información consolidada de todos los activos de las dependencias al Encargado o encargados asignados para gestionar la seguridad de la información,	Funcionarios Enlaces responsables o encargados de las diferentes dependencias	Correo electrónico
6. Realizar la revisión técnica de los activos de	Validar que la matriz haya sido diligenciada	Encargado o encargados asignados para gestionar la	

información	correctamente de acuerdo a las indicaciones dadas.	seguridad de la información,	Matriz de activos de información revisada
¿Requiere ajustes?	Si: Pasa a la actividad 7 No: Pasa a la actividad 8		
7. Realizar ajustes solicitados	Realizar los ajustes solicitados por Encargado o encargados asignados para gestionar la seguridad de la información,	Usuario/funcionarios	Matriz de activos de información ajustes
8. Consolidar las matrices de activos de información de todas las dependencias en un solo archivo	Realizar la consolidación de todas las matrices de activos de información en un solo archivo.	Encargado o encargados asignados para gestionar la seguridad de la información.	Matrices de activos de información por dependencias en un solo archivo.
9. Remitir el archivo consolidado de activos de información a la Dirección de Sistemas	Enviar la matriz de activos de información consolidada a la persona asignada por la Oficina de Sistemas.	Encargado o encargados asignados para gestionar la seguridad de la información.	Correo electrónico
10. Gestionar la publicación de los activos de información en los portales que corresponda.	Gestionar la publicación de los activos de información de acuerdo a los requerimientos legales nacionales e internos.	Responsable Oficina de Sistemas	Publicación en portales correspondiente
fin			

Tabla 11. Procedimiento de las actividades para levantamiento de matriz de activos de información en la entidad

Fuente: Elaboración propia

Diagrama del Procedimiento

La Figura 9 representa el procedimiento para el levantamiento de matriz de activos de información en la entidad descrita anteriormente, esta figura se podrá observar con mayor claridad en el Anexo_ 19_Diagrama Flujo Procedimiento.

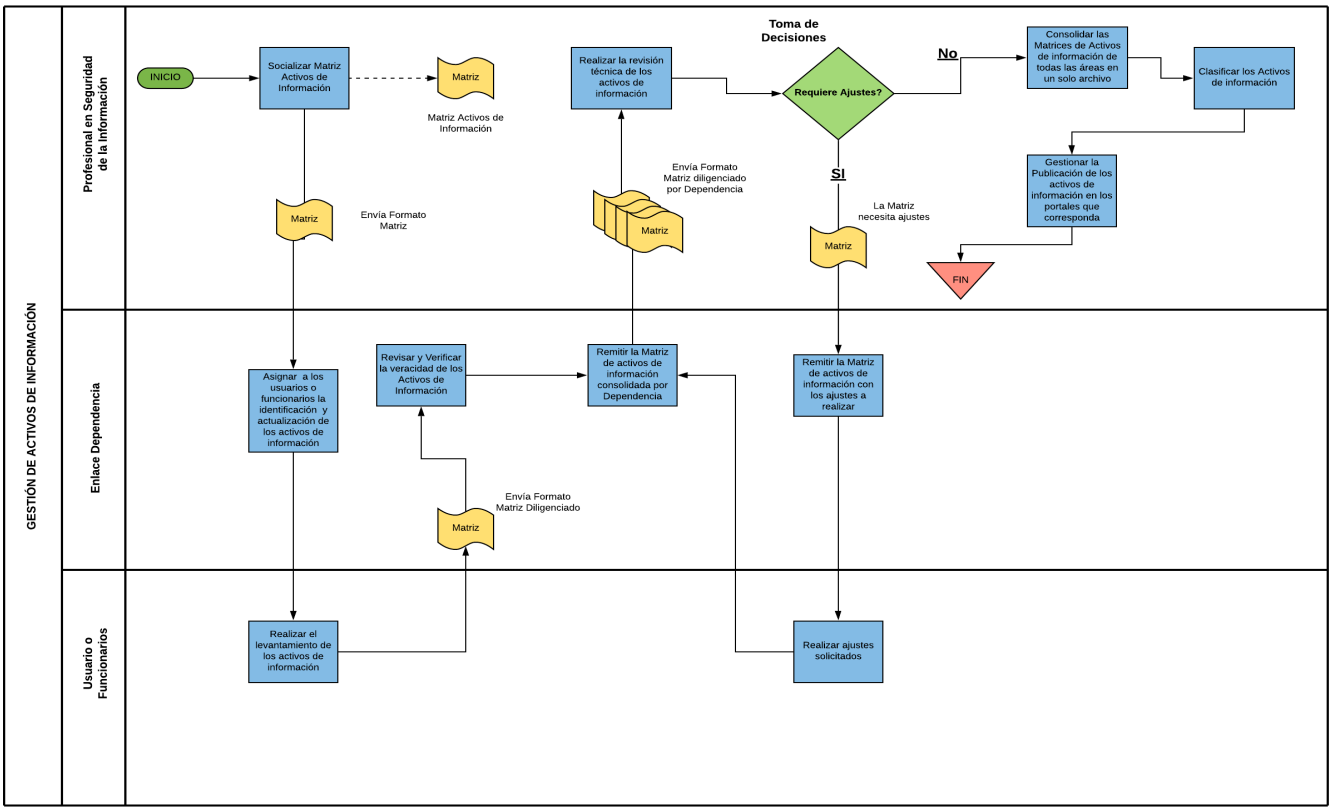


Figura 9. Diagrama del procedimiento

Fuente: Elaboración propia

PASO 3 - CONSOLIDADO GENERAL DE ACTIVOS DE INFORMACIÓN

Una vez se ha realizado el diligenciamiento de la matriz de activos de información por cada una de las dependencias o áreas de la organización, se prestará especial atención a la casilla marcada **"Nivel de Criticidad"** y se seleccionarán los activos con importancia superior, marcados con nivel alto y crítico, estos a su vez, se consolidarán en un único formato que se encuentra en el Anexo_21_Matriz Clasificación de Activos, este formato llevará el código de identificación del activo, nombre, nivel de criticidad y contenedor; a cada activo de información se le debe asociar un contenedor según corresponda, cabe resaltar que estos son genéricos a las entidades, en caso de optar por otro tipo de contenedor u otro nombre, esta metodología permitirá incluirlo en su desarrollo.

Contenedores de los activos de información: Los contenedores hacen referencia a la generalización de los activos de información según, la casilla de la matriz de levantamiento

de activos marcada como ubicación física y/o digital, si los activos de información comparten similitudes en su ubicación física o digital se asocian a un contenedor, esto con el fin de diferenciar y organizar los activos de información de forma general; a continuación, se mencionan algunos contenedores genéricos.

- Información digital en unidad de disco backup (D o G.)
- Intranet (información)
- Información digital disco (unidad C)
- Información digital disco (escritorio)
- Sistemas de Información Externos (software / aplicativos)
- Sistemas de Información Internos (software / aplicativos)
- Sitios Web (externos / internos)
- Información Física (carpetas, papel, archivadores)
- Redes Sociales (Twitter, Facebook, Instagram)
- Servidores de Datos
- Servidores de Aplicaciones
- Almacenamiento externo (CD, DVD, USB, HHDD)
- Almacenamiento en la nube (Google drive, Dropbox, OneDrive, plataformas)
- Correo electrónico
- Servicios de comunicación (chat, voz, video)
- Almacenamiento en dispositivos móviles (Smartphone, tabletas)
- Dispositivos Hardware (impresoras, plotter, scanner)
- Otros, que el encargado o encargados de la seguridad consideren necesarios

Una vez se ha diligenciado el formato “clasificación de activos” (Figura 10), se procede a seleccionar los activos que se encuentran en nivel de criticidad “Crítico”, en este punto, se deben filtrar y agrupar los contenedores comunes de los activos de información en una hoja

de cálculo diferente, este mismo procedimiento se debe realizar con los activos de criticidad "Alta"; esta clasificación será el insumo para el análisis de riesgos de los activos de información.

CLASIFICACION DE ACTIVOS			
Codigo Identificacion del Activo	Nombre del Activo	Nivel de Criticidad	Contenedor y/o Activo de informacion Seleccionado para analisis de riesgos
SJ-001	PROCESOS ORDINARIOS	Alta	Informacion Digital Disco Backup (D o G)
SJ-002	PROCESOS CONSTITUCIONALES	Crítica	Informacion Digital Disco Backup (D o G)
SJ-003	PONENCIAS	Alta	Informacion Digital Disco Backup (D o G)
SJ-004	INFORMES	Alta	Informacion Fisica en Archivador
SJ-005	CUADRO DE MIS PROCESOS	Alta	Informacion Digital Disco Backup (D o G)
SJ-009	PROCESOS POLICIVOS	Crítica	Informacion Digital Disco Backup (D o G)
SJ-012	PROCESOS ORDINARIOS	Alta	Informacion Digital Disco Backup (D o G)
SJ-013	PROCESOS CONSTITUCIONALES	Crítica	Informacion Digital Disco Backup (D o G)
SJ-014	PONENCIAS COMITÉ DE CONCILIACIÓN	Alta	Informacion Digital Disco Backup (D o G)
SJ-015	INFORMES	Crítica	Informacion Digital Disco Backup (D o G)
SJ-016	CUADRO DE MIS PROCESOS	Alta	Informacion Digital Disco Backup (D o G)
SJ-017	PROCESOS ORDINARIOS	Alta	Informacion Digital Disco (C ó Escritorio)
SJ-018	COMITÉ DE CONCILIACION	Alta	Informacion Digital Disco (C ó Escritorio)
SJ-019	PROCESOS ORDINARIOS	Alta	Informacion Digital Disco Backup (D o G)
SJ-020	PROCESOS CONSTITUCIONALES	Crítica	Informacion Digital Disco Backup (D o G)
SJ-021	PROCESOS PENALES	Alta	Informacion Digital Disco Backup (D o G)
SJ-022	PONENCIAS COMITÉ DE CONCILIACIÓN	Crítica	Informacion Digital Disco Backup (D o G)
SJ-023	TODOS LOS INFORMES JURIDICA	Crítica	Informacion Digital Disco Backup (D o G)
	CONSOLIDADO PROCESOS JURIDICA		

Figura 10. Formato clasificación de activos

Fuente: Elaboración propia

Como se mencionó en el paso 3, en esta etapa del proceso se debe contar con una clasificación de activos de información agrupada en contenedores generales, estos permitirán que se pueda realizar un análisis de riesgos de una forma asertiva, ágil y precisa guardando las prioridades e importancia de los activos de información de la entidad.

El análisis de riesgos tiene como propósito identificar, documentar y proteger los activos de información de la entidad de posibles riesgos a los que pueden estar expuestos y que alteren factores como: su integridad, disponibilidad y confidencialidad, de esta forma se busca evitar, reducir, compartir o asumir los riesgos detectados. Esta metodología le permitirá al lector desarrollar el análisis de riesgos de su entidad de una forma completa, teniendo presente la normatividad vigente y los lineamientos gubernamentales expuestos en el MSPI, para esto, se ha desarrollado una matriz de riesgos, donde se consignará la información referente a los activos de información, sus riesgos y controles.

CAPÍTULO 2.

GESTIÓN DEL RIESGO

GENERALIDADES

Esta metodología comprende las etapas para realizar el inventario de activos y la identificación de riesgos de seguridad de la información, que incluyen: la información de activos en contenedores, la identificación del riesgo, el análisis del riesgo y la definición de controles, aplica a los activos de información con criticidad "crítica y alta", sin embargo, si la entidad decide realizar un análisis de riesgos a todos sus activos, se deben incluir los contenedores de los activos con criticidad "media y baja", todos los procesos desarrollados en esta metodología están acordes con los lineamientos establecidos en la Norma NTC-ISO/IEC 27001:2013, la implementación de los controles respectivos para los riesgos existentes está acorde con lo descrito en la guías 5 y 7 del Modelo de seguridad y privacidad de la información del MinTIC.

Mejores Prácticas según la Norma ISO 27002

La parte principal de la norma ISO 27002 se encuentra distribuida en las siguientes secciones, que corresponden a controles de seguridad de la información. Es importante recordar que la entidad puede utilizar esas directrices como base para el desarrollo del SGSI.

2. **Sección 5 – Política de Seguridad de la Información**

Se debe elaborar un documento acerca de la política de seguridad de la información de la empresa, que deberá establecer los conceptos de seguridad de la información, una estructura para establecer los objetivos y las formas de control, el compromiso de la dirección con la política, entre otros factores.

3. **Sección 6 – Organización de la Seguridad de la Información**

Para implementar la Seguridad de la Información en la entidad, se hace indispensable contar con una estructura para gestionarla de una manera adecuada. Para ello, las actividades de seguridad de la información tienen que ser dirigidas por representantes de la organización, que deben contar con compromisos bien definidos y proteger la información de carácter confidencial.

4. **Sección 7 – Gestión de activos**

Activo, según la norma, es cualquier elemento que tenga valor para la organización y que necesite ser protegido. Pero para ello los activos deben ser identificados y clasificados, d manera tal que un inventario pueda ser estructurado y posteriormente mantenido; además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos.

5. **Sección 8 – Seguridad en recursos humanos**

Antes de la contratación de un empleado – o incluso de proveedores – es importante que sea correctamente analizado, principalmente si se trata de información de carácter confidencial. La intención de esta sección es disminuir el riesgo de fraude, robo o mal uso de los recursos; y cuando el empleado esté trabajando en la empresa, debe ser consecuente ante las amenazas a la seguridad de la información, así como de sus responsabilidades y obligaciones.

6. **Sección 9 – Seguridad física y del medio ambiente**

Los equipos e instalaciones donde se procesa información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales.

7. **Sección 10 – Seguridad de las operaciones y comunicaciones**

Es importante que estén definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información. Esto incluye la gestión de servicios a terceros, la planificación de recursos de los sistemas para minimizar el riesgo de fallas, la creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración segura de las redes de comunicaciones.

8. **Sección 11 – Control de acceso**

El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera.

9. **Sección 12 – Adquisición, desarrollo y mantenimiento de sistemas**

Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos.

10. **Sección 13 – Gestión de incidentes de seguridad de la información**

Los procedimientos formales de registro y escalonamiento deben ser establecidos y los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil.

11. **Sección 14 – Gestión de continuidad del negocio**

Los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas.

12. **Sección 15 – Conformidad**

Es importante evitar la violación de cualquier ley criminal o civil, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información. En caso necesario, la empresa puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios.

DEFINICIONES

Los términos y definiciones aplicables para la identificación de riesgos de Seguridad de la Información se basan en la Norma NTC-ISO/IEC 27000:2013.

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo con base en su probabilidad e impacto de ocurrencia.

Autenticidad: Propiedad de que una Organización es lo que afirma ser.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, o ejecutar procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de Seguridad de la Información por debajo del nivel de

riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. También se puede definir como una medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona/organización autorizada. La información debe estar en el momento y en el formato que se requiera, al igual que los recursos necesarios para su uso. La no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los usuarios de la organización.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de Seguridad de la Información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de incidentes de Seguridad de la Información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Proceso efectuado por la alta dirección de la organización y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: El costo para la organización de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros, como pérdida de reputación o implicaciones legales.

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Incidente de seguridad de la información: Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la organización debe ser con calidad, clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información puede exponer a la organización a toma de decisiones incorrectas, lo cual puede tener impacto reputacional, financiero y/o legal.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de Seguridad de la Información inaceptables e implantar los controles necesarios para proteger la información.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona u organización con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Responsable de Seguridad Informática: En la organización, la Dirección de TI será encargado de realizar el seguimiento y monitoreo al Subsistema de Gestión de la Seguridad de la información (SGSI).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

Sistema de Gestión de la Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer la política y los objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Seguridad de la Información: Preservación de los principios de confidencialidad, la integridad y la disponibilidad de la información.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

LINEAMIENTOS

Las entidades públicas como organismos gubernamentales tienen la misión de garantizar el bienestar general y el mejoramiento de la condición de vida de sus habitantes, a través de la prestación de servicios de calidad, en cumplimiento de las competencias definidas en la constitución política y demás normas complementarias, acatando los requisitos legales y organizacionales suscritos frente al Sistema Integrado de Gestión (SIG) en materia de administración de los riesgos institucionales y de corrupción.

Comprendiendo la importancia de una adecuada gestión de riesgos y como parte fundamental del subsistema de seguridad de la información, Las entidades deben contar con instrumentos para la identificación y análisis de riesgos de seguridad y privacidad de la información, esta metodología es uno de ellos.

En esta etapa del proceso de la metodología propuesta, se tiene a disposición del lector y de su entidad, una matriz de riesgos de los activos de información, esta se debe diligenciar en su totalidad considerando los aspectos que refieren a las vulnerabilidades y riesgos que lleguen a existir, cabe resaltar que el mantenimiento y continuidad del inventario y clasificación de activos de información y su análisis de riesgos son elementos fundamentales para lograr la optimización de los procesos y procedimientos de la organización.

Para poder desarrollar y gestionar la matriz de riesgos, se debe contar con insumos que se presentan a continuación: el formato de clasificación de la información y sus respectivos contenedores de activos totalmente diligenciado, además de tener claridad sobre los procesos y procedimientos que se llevan al interior de la organización.

A continuación, esta metodología presenta lineamientos que le permitirán al encargado o encargados de la seguridad de la información seguir un orden adecuado en el análisis de riesgos de su entidad y así tener las bases para implementar el sistema de gestión de la seguridad de la información.

Establecer el líder del Proceso

El primer paso será establecer el líder, a través de un acta de nombramiento se debe elegir democráticamente al líder del proceso, el perfil de este líder debe ser un profesional universitario en sistemas, electrónica, telecomunicaciones, informática, o áreas afines, preferiblemente con grado de especialización y certificación en la norma ISO 27001:2015, también puede ser el funcionario existente en la entidad responsable de organizar y gestionar el área de desarrollo de sistemas informáticos, el líder elegido estará en compañía de un grupo interdisciplinario comprometidos con el análisis de riesgos e implementación de controles a los riesgos detectados.

Grupo Interdisciplinario

En secuencia, se debe conformar un grupo interdisciplinario, la idea de este grupo y su integralidad es aportar al tratamiento de los riesgos una visión completa de la entidad y la cual se pueda tener la participación de diferentes áreas estudiando un mismo proceso, es importante y ayuda a enfocar correctamente el modelo de la seguridad de la información, es por esta razón que se deben incluir los riesgos de seguridad de la información en el momento que se hace el análisis para el modelo estándar de control interno, o para el modelo de gestión de calidad.

Capacitación

La capacitación en temas relacionados con seguridad de la información en la metodología son importantes, porque es evidente que el grupo interdisciplinario debe instruirse para poder estudiar ahora los riesgos de seguridad de la información, sin embargo el grupo debe estar complementado por alguno de los encargados de la seguridad de la información, para que los pueda orientar, con este grupo interdisciplinario se puede tener un contexto organizacional amplio en diferentes aspectos del desarrollo del análisis de riesgos.

Evidenciar

Se deberá evidenciar el nombramiento del líder, del grupo interdisciplinario, su capacitación y todas aquellas situaciones que se presenten durante el proceso de análisis de riesgos expuesto en esta metodología.

Mapa de Proceso de Análisis de Riesgos

Se debe conocer el mapa de proceso de análisis de riesgos, este será la guía para avanzar paso a paso y llegar a desarrollar completamente el análisis propuesto en esta metodología.

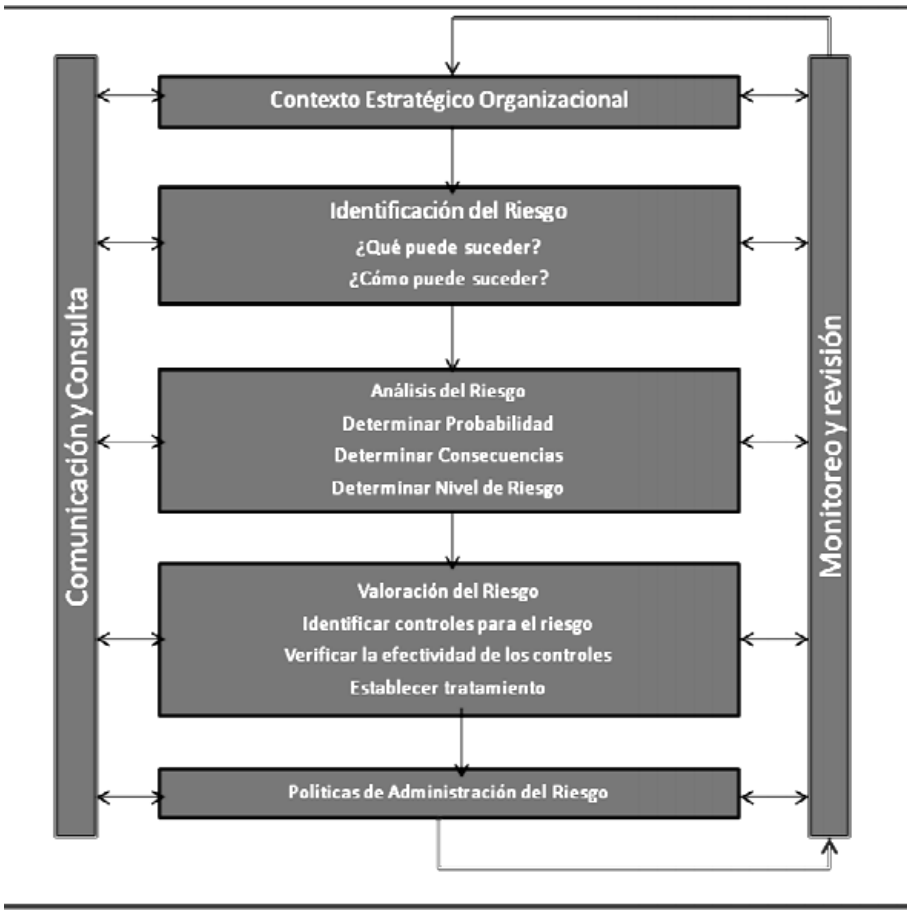


Figura 11. Mapa de proceso de análisis de riesgos

Fuente: Guía No 7 MINTIC

DESARROLLO

CONTEXTO ESTRATÉGICO ORGANIZACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Una vez se han seguido los pasos anteriores se debe revisar el contexto estratégico organizacional de seguridad y privacidad de la información, a continuación, se describen aspectos importantes.

El contexto estratégico organizacional de seguridad y privacidad de la información, hace referencia al conocimiento de las cuestiones internas y externas que afectan a la entidad, por tanto la información de las entidades del estado colombiano es muy importante para el desarrollo de su objeto misional enmarcado en el bienestar de la ciudadanía, es por ello que debe ser salvaguardada ante la posibilidad de que suceda algún evento de riesgo en

seguridad de la información y que pudiese generar un impacto crucial, generando de allí una consecuencia negativa para el normal progreso de las actividades de la organización.

De acuerdo con lo anterior y tomando como referencia el Modelo de Seguridad y Privacidad de la información (MSPI) de MINTIC se tiene que:

Las entidades deberán contar con la política de administración de riesgos en el sistema integrado de gestión de calidad, el cual tiene como objetivo:

Generar una cultura de conocimiento y manejo de los riesgos que prevengan la ocurrencia de situaciones o eventos que tengan un impacto o consecuencia sobre el cumplimiento de la misión u objetivos institucionales, generando un ambiente de control al interior de la organización, con el fin de garantizar el cumplimiento de la constitución y la ley.

Es determinante definir el propósito de la gestión del riego en la seguridad de la información y su alcance, pues estas condiciones afectan a los procesos, específicamente, al establecimiento del contexto.

Este propósito puede ser:

- ✓ Brindar soporte al modelo de seguridad de la información a la entidad.
- ✓ Elaboración de un plan de respuesta a incidentes.
- ✓ Realización de los estudios en seguridad de la información para un producto un servicio.
- ✓ En consecuencia de la definición del contexto estratégico es la consolidación de criterios fundamentales como: límites, alcance y organización del proceso de gestión de riesgos en la seguridad de la información.

El contexto estratégico se tiene en cuenta en el proceso desde el inicio, esto se debe a la necesidad de tener certeza en el contexto en el cual se desplegará el proyecto, precisando el ambiente en el que se desarrollará, qué procesos incluirá, cual es movimiento de dicho o dichos procesos, y de esta forma determinar su alcance y objetivos, finalmente, de allí conseguir los riesgos de seguridad relacionados. De igual forma el grupo interdisciplinar, tiene ventajas como conocer los modelos de gestión establecidos en la entidad, analizando los flujos de procesos ya identificados, para aportar su visión desde el análisis de riesgos de la entidad.

Cuando se establezca el contexto estratégico organizacional de seguridad y privacidad de la información se sugiere tener en cuenta las cuestiones internas y externas, a continuación, algunos contextos que se deben tener en cuenta:

Contexto Externo

- **Económicos:** incrementos salariales de obligación legal, impuestos y gravámenes.
- **Medioambientales:** energía, desarrollo sostenible, catástrofes naturales, emisiones y residuos.
- **Políticos:** Cambios de gobierno, regulación, políticas públicas, legislación.
- **Sociales:** responsabilidad social, demografía, terrorismo.
- **Tecnológicos**: comercio electrónico, datos externos, interrupciones, tecnología emergente.

Contexto Interno

- **Infraestructura:** acceso al capital, capacidad de los activos, disponibilidad de activos.
- **Talento Humano:** salud, capacidad del personal, seguridad.
- **Procesos:** capacidad, proveedores, entradas, diseño ejecución, salidas, conocimiento.
- **Tecnología:** disponibilidad de datos y sistemas, desarrollo, integridad de datos, producción, mantenimiento.

Por tanto, el líder, el equipo interdisciplinar y los encargados de la seguridad de la información serán los llamados a definir un contexto estratégico organizacional, basados en las estrategias que permitan encaminar a la entidad en la búsqueda y consolidación de excelentes resultados en la gestión del riesgo.

Es trascendental que la entidad defina el alcance y los límites así de esta manera garantizar que todos los activos principales se tomen respecto a la valoración del riesgo.

Alcance

Al definir el alcance y los límites la entidad debería considerar la siguiente información:

- ✓ Objetivos de negocio, estrategias de la organización y políticas.
- ✓ Procesos y procedimientos del negocio.
- ✓ Estructura de la organización y funciones.
- ✓ Las obligaciones y requisitos legales, reglamentarios aplicables a la organización.
- ✓ La política de seguridad de la información.

- ✓ La perspectiva de la organización hacia la gestión del riesgo.
- ✓ Activos de información.
- ✓ Lugar geográfico de la organización y sus características.
- ✓ Prohibiciones que afectan a la organización.
- ✓ Intereses de terceros y de las partes interesadas.
- ✓ Medio sociocultural.
- ✓ Interfaces de cambio con otras entidades

Enfoque

Se pueden aplicar diferentes enfoques, según lo determine el grupo interdisciplinar, sin embargo, debe contar con criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo.

Criterios de evaluación del riesgo

Esta metodología sugiere armar criterios para la evaluación del riesgo con el fin de establecer el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos:

- El valor del proceso de información para la entidad
- El valor de la criticidad de los activos de información.
- Los requisitos legales y reglamentarios.
- La relevancia de la disponibilidad de la, confidencialidad, e integridad de la información para los procesos de la entidad.

Criterios de impacto

Se sugiere establecer criterios de impacto del riesgo y traducirlos en términos del nivel de perjuicio o de los costos para la entidad, causados por un suceso de seguridad de la información, considerando los siguientes aspectos:

- Grado de clasificación de los activos de información de los procesos
- Quebrantos de la seguridad de la información (pérdidas de confidencialidad, integridad y disponibilidad)
- Operaciones descontinuadas

- Desgaste de valor financiero
- Variación de planes y fechas limites
- Perjuicios para la reputación
- Violación de los requisitos legales.

Criterios de aceptación del riesgo

Se sugiere desarrollar y detallar los criterios de aceptación del riesgo. Estos criterios obedecen con frecuencia a las políticas, metas, objetivos de la entidad, la entidad deberá puntualizar sus propias escalas para los niveles de aceptación del riesgo. Sin embargo, es acertado considerar los siguientes aspectos:

- ✓ Los criterios de aceptación del riesgo pueden contener múltiples umbrales, con una meta de nivel de riesgo deseable, aceptados por la entidad.
- ✓ Los criterios de aceptación del riesgo se pueden formular como la relación entre el beneficio estimado y el riesgo estimado.
- ✓ Los diferentes criterios de aceptación del riesgo pueden estar asociados a diferentes clases de riesgos.
- ✓ Los criterios de aceptación del riesgo pueden contener requisitos para tratamiento adicional en el futuro.

IDENTIFICACIÓN DE RIESGOS

Una vez establecido el contexto estratégico organizacional de seguridad y privacidad de la información, el líder del proceso, los encargados de la seguridad de la información y el grupo interdisciplinar, deberán realizar una serie de encuentros estratégicos y reuniones programadas, donde el objetivo será la identificación de los riesgos que se pudiesen presentar los contenedores de los activos de información asociados a los procesos descritos en la matriz de levantamiento de activos de información. En esta etapa del proceso se deben plantear las siguientes preguntas: **¿Qué puede suceder?, ¿Cómo puede suceder?**

De acuerdo con lo planteado en esta metodología, la identificación del riesgo se realiza basándose en las causas identificadas en los procesos, estas causas pueden ser internas o externas, según lo que la entidad haya encontrado a través del contexto estratégico.

En este instante es significativo establecer cuáles son los activos críticos para asociarlos a los procesos adecuados y de allí generar el listado de procesos críticos, inventariar los activos de información sensible, mantener actualizada la clasificación de activos con criticidad **"crítica y alta**", es importante la participación del grupo interdisciplinar en compañía de los

encargados de la seguridad de la información y el líder del proceso, donde se revisarán los procesos y los contendores de los activos de información, tomando parte en la identificación de los riesgos de seguridad, para los activos que pertenecen a procesos que se identifican como críticos dentro del planteamiento del MSPI.

Esta guía metodológica insiste con la definición de algunos términos que son necesarios para la identificación de los riesgos, estos términos son comúnmente usados en las entidades para efectos de la aplicación del sistema de calidad, modelo de control interno y se listarán a continuación:

- **Definición de Riesgo**

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la *"Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias"*. De igual manera, el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información de la organización.

De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital, atendiendo a la guía 7 Gestión de Riesgos del MSPI, Modelo de Seguridad y Privacidad de la Información, se busca en esta metodología la identificación, análisis y generación de controles de los riesgos de seguridad y privacidad de la información.

- **Riesgos de Ciberseguridad:**

Riesgos que resultan de la composición de amenazas y vulnerabilidades en el ambiente digital y por su naturaleza cambiante incluye también características relacionadas con el entorno físico; estos riesgos tienen una correlación puntual con los principios de la seguridad de la información y se clasifican teniendo en cuenta los siguientes grupos:

a. Pérdida de la Confidencialidad: Pérdida de propiedades de la información que imposibilita su divulgación a individuos, también se ve reflejado en procesos sin autorización.

b. Pérdida de la Integridad: Pérdida de características para establecer información exacta y completa, pudo haber sido manipulada o alterada por personas o procesos sin autorización.

c. Pérdida de la Disponibilidad: Pérdida de la condición de la información de encontrarse asequible para quienes requieran acceder a ella, ya sean personas, procesos o aplicaciones.

- **Riesgos de Seguridad y Privacidad de la Información**

Riesgos que aquejan a las personas donde sus datos no son bien tratados y se genera una posible violación de sus derechos, la pérdida de información necesaria o el perjuicio causado por una utilización ilícita o fraudulenta de los mismos.

En concordancia con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como *"Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y vulnerar la seguridad"*; por lo tanto, se representarían en riesgos de seguridad y privacidad de la información, como es el riesgo de tener un uso no apropiado de la información personal, lo que resulta en una violación de los derechos constitucionales.

Para la identificación, análisis y valoración de los riesgos de seguridad de la información, se tomó como base la matriz de activos de información, la cual establece los niveles de criticidad de los activos, además del formato y algunas características importantes que permiten su clasificación, con este propósito, es necesario coordinar las acciones y procesos con el grupo interdisciplinar, con los encargados de la seguridad de la información y con el líder del proceso de análisis de riesgos.

- **Proceso:** Son una serie de actividades relacionadas entre ellas y que interactúan para generar valor, las cuales convierten elementos de entrada en resultados (productos/servicios) de acuerdo a las exigencias de la ciudadanía o partes interesadas.

- **Objetivo del Proceso:** Consiste en definir los patrones diferenciadores de los procesos (proveedores, salidas, insumos, clientes y riesgos asociados), hace ver de manera íntegra y secuencial la condición del proceso y el aporte que hace a los objetivos institucionales.

- **Identificación de Activos:** La identificación de activos de información, permite seleccionar los activos a los que se les debe ofrecer mayor protección, identifica claramente sus características y rol al interior de un proceso.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para ocasionar una pérdida o perjuicio en un activo de información. Suele referirse como una combinación de la probabilidad de un acontecimiento y sus consecuencias.

- **Causas (Amenazas y Vulnerabilidades):** Los fundamentos o el origen de una situación determinada. La causa es el primer elemento a partir del cual se desarrollan acontecimientos o situaciones específicas.

- **Descripción del Riesgo:** es la información detallada del riesgo que define y limita una condición adversa para la toma de decisiones.

• **Efectos de la materialización del Riesgo**: Una vez materializado el riesgo, solo queda la mejor gestión posible desde el punto de vista estratégico y de riesgos, que permitan la recuperación parcial o total de los recursos comprometidos.

Una vez se han identificado los riesgos esto se deben clasificar según su impacto, y los efectos y consecuencias que pueden traer a la entidad, esta guía metodológica permitirá agregar los que la entidad considere pertinentes, sin embargo, se presentan las siguientes opciones:

- ✓ Riesgo Estratégico: se enfocan a asuntos generales asociados con la misión, visión y el cumplimiento de los objetivos estratégicos.
- ✓ Riesgos de Imagen: están relacionadas con la apreciación y la confianza por parte de los ciudadanos hacia la entidad.
- ✓ Riesgos Operativos: Asociadas al funcionamiento y operación de los sistemas de información propios de la entidad, al cumplimiento de los objetivos de los procesos y la interacción entre estos.
- ✓ Riesgos Financieros: Corresponden al manejo de los recursos de la organización que incluyen la ejecución presupuestal, la preparación de los estados financieros, los pagos, administraciones de excedentes de tesorería y el manejo sobre los bienes.
- ✓ Riesgos de Cumplimiento: Se relacionan con la preparación de la organización para cumplir con los requisitos legales, contractuales, de ética y en general con su responsabilidad ante las partes interesadas.
- ✓ Riesgos de Tecnología: Se asocian con la capacidad tecnológica de la organización para cumplir sus necesidades actuales y futuras y el desarrollo de la misión.

Esta metodología permitirá incluir los riesgos de seguridad que considere pertinentes teniendo en cuenta siempre como los riesgos podrían la afectar la confidencialidad, integridad y disponibilidad de la información según su nivel de criticidad.

ANÁLISIS DE RIESGOS

El siguiente paso establece que una vez se han identificado los riesgos se procede a su análisis, este es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir a los activos de información de la entidad, es de suma importancia documentar y evidenciar cada una de las etapas

realizadas para el proceso de análisis de riesgos, de allí la entidad tendrá sus propias herramientas para poder replicar este mismo procedimiento.

A continuación, se plantean una serie de etapas para la generación del análisis de riesgos de las entidades, basadas la norma ISO27005.

Identificación Del Riesgo

El propósito de la identificación del riesgo es establecer qué podría causar una pérdida potencial, de ahí llegar a comprender ¿cómo?, ¿dónde?, ¿por qué? podría ocurrir está pérdida, estos interrogantes permiten recolectar datos de entrada para esta actividad.

Identificación de Los Activos

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, necesita de protección. La identificación de activos a este punto de la metodología debe estar consolidada en la matriz de activos y clasificada según lo expuesto en la primera parte.

Identificación de Amenazas

Una amenaza tiene el potencial de causar daños en especial a los activos de información que hacen parte fundamental del planteamiento de esta metodología, además, procesos y sistemas de la entidad. Las amenazas pueden ser originadas de forma natural o por el humano y podrían ser accidentales o intencionales, es recomendable enfocar todos los orígenes de las amenazas.

Las amenazas pueden perturbar a más de un activo y pueden ocasionar diferentes impactos dependiendo de los activos que se vean involucrados.

A continuación, se listan una serie de amenazas comunes según la ISO 27001

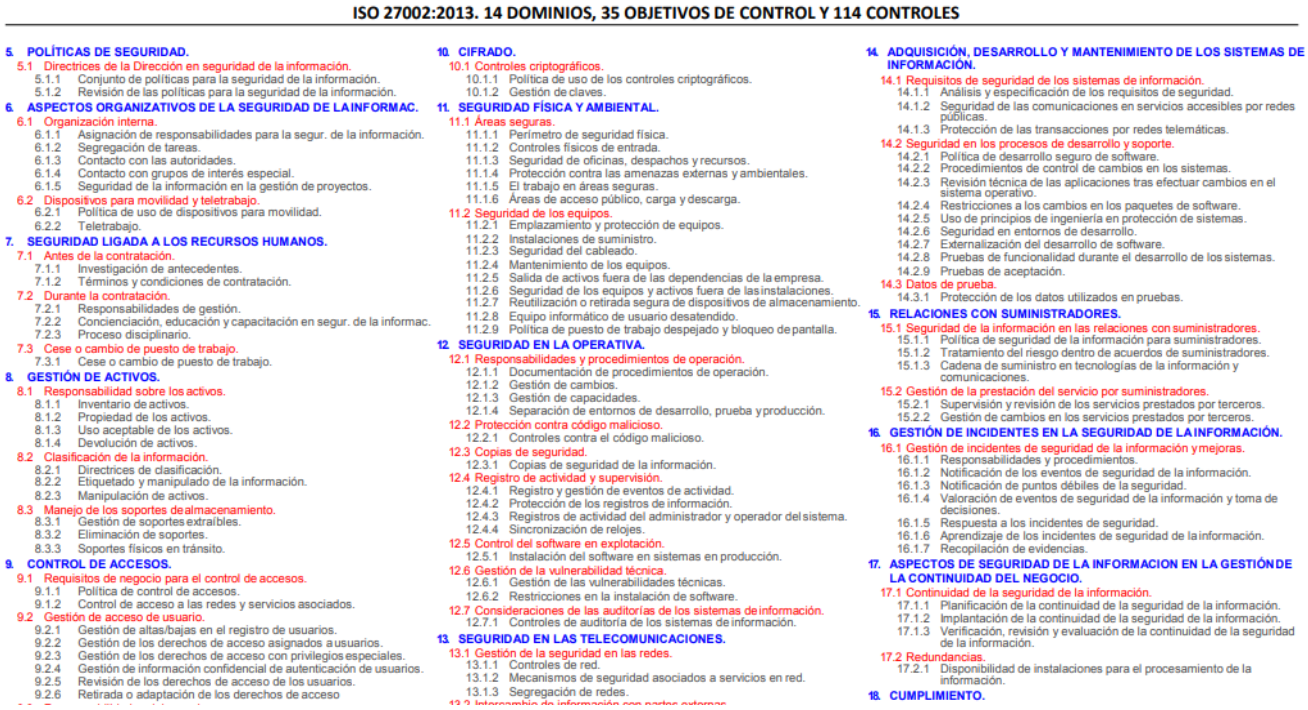
- Acceso a la red o al sistema de información por personas no autorizadas.
- Amenaza o ataque con bomba.
- Incumplimiento de relaciones contractuales.
- Infracción legal.
- Comprometer información confidencial.
- Ocultar la identidad de un usuario.
- Daño causado por un tercero.
- Daños resultantes de las pruebas de penetración.
- Destrucción de registros.
- Desastre generado por causas humanas.
- Desastre natural, incendio, inundación, rayo.
- Divulgación de contraseñas.
- Malversación y fraude.
- Errores en mantenimiento.
- Fallo de los enlaces de comunicación.
- Falsificación de registros.
- Espionaje industrial.
- Fuga de información.
- Interrupción de procesos de negocio.
- Pérdida de electricidad.
- Pérdida de servicios de apoyo.
- Mal funcionamiento del equipo.
- Código malicioso.
- Uso indebido de los sistemas de información.
- Uso indebido de las herramientas de auditoría.
- Contaminación.
- Errores de software.
- Huelgas o paros.
- Ataques terroristas.
- Hurtos o vandalismo.
- Cambio involuntario de datos en un sistema de información.
- Cambios no autorizados de registros.
- Instalación no autorizada de software.
- Acceso físico no autorizado.
- Uso no autorizado de material con copyright.
- Uso no autorizado de software.
- Error de usuario.
- Revelación de información.

Identificación de Controles

Se debe ejecutar la identificación de los controles que existen para minimizar trabajo o costos innecesarios, por dar ejemplo: controles duplicados o controles descontinuados, además de esto mientras se identifican los controles se recomienda hacer una comprobación para avalar que los existentes funcionan correctamente.

Esta metodología está soportada en las normas ISO en especial la norma ISO/IEC 27002:2005 norma internacional que establece el código de mejores prácticas para apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones y plantea 11 dominios, 39 objetivos de control y 133 controles, sin embargo si algún control que se desea aplicar no está contemplado en la norma ISO 27002, la entidad podrá establecer sus propios controles según el contexto organizacional. En el Anexo_20_Controles_Iso27002-2013, se encontrará el listado de controles según la norma mencionada.

A continuación, se ilustran los controles planteados en la norma ISO27002.



ISO 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LAINFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

Figura 12. Controles según ISO 27002

Fuente: Norma ISO 27002

Identificación de Vulnerabilidades

Las vulnerabilidades son defectos o debilidades en un activo que le permite a un atacante vulnerar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

A continuación, se listan una serie de vulnerabilidades comunes según la norma ISO 27001.

- interfaz de usuario complicada.
- Contraseñas predeterminadas no modificadas.
- Eliminación de medios de almacenamiento sin eliminar datos.
- Sensibilidad del equipo a los cambios de voltaje.
- Sensibilidad del equipo a la humedad, temperatura o contaminantes.
- Inadecuada seguridad del cableado.
- Inadecuada gestión de capacidad del sistema.
- Gestión inadecuada del cambio.
- Clasificación inadecuada de la información.
- Protección física no apropiada.
- Reemplazo inadecuado de equipos viejos.
- Falta de formación y conciencia sobre seguridad.
- Inadecuada segregación de funciones.
- Mala segregación de las instalaciones operativas y de prueba.
- Insuficiente supervisión de los empleados y vendedores.
- Especificación incompleta para el desarrollo de software.
- Pruebas de software insuficientes.
- Falta de política de acceso o política de acceso remoto.
- Desprotección en equipos móviles.
- Falta de redundancia, copia única.
- Ausencia de sistemas de identificación y autenticación.
- No validación de los datos procesados.
- Ubicación vulnerable a inundaciones.
- Mala selección de datos de prueba.
- Copia no controlada de datos.
- Descarga no controlada de Internet.
- Uso incontrolado de sistemas de información.
- Software no documentado.

- Control inadecuado del acceso físico.
- Mantenimiento inadecuado.
- Inadecuada gestión de red.
- Respaldo inapropiado o irregular.
- Inadecuada gestión y protección de contraseñas.
- Ausencia de política de escritorio limpio y pantalla clara.
- Falta de control sobre los datos de entrada y salida.
- Falta de documentación interna.
- Carencia o mala implementación de la auditoría interna.
- Falta de políticas para el uso de la criptografía.
- Empleados desmotivados.
- Conexiones a red pública desprotegidas.
- Los derechos del usuario no se revisan regularmente.
- Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.

EVALUACIÓN DE RIESGOS

Para la evaluación del riesgo es importante contar con la información obtenida en la fase anterior "análisis de riesgos (amenazas y vulnerabilidades)", por tanto, la entidad debe diseñar los criterios de riesgo delimitando los niveles de riesgo aceptados por la misma.

De esta forma se debe analizar la "probabilidad e impacto" que los riesgos pudiesen ejercer en los activos de información, por ello es de importancia conocer a que hacen referencia.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Determinación de la Probabilidad del Riesgo

En la siguiente tabla se establece la forma en que se determina la probabilidad del riesgo.

Nivel	Descriptor	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	Posible	El evento probablemente podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos 1 vez en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Tabla 12. Determinación de la probabilidad del riesgo

Fuente: Guía No 7 MINTIC

Impacto: se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo".

Determinación de la Probabilidad del Impacto

En la siguiente tabla se establece la forma en que se determina la probabilidad del impacto

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 13. Determinación de la probabilidad del impacto.

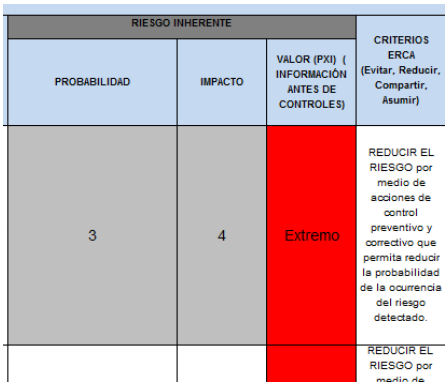
Fuente: Guía No 7 MINTIC

La valoración del riesgo se hace de manera cualitativa realizando una comparación donde se presenta el análisis de la probabilidad de ocurrencia del riesgo contra el impacto del mismo, consiguiendo al final la matriz denominada “Matriz de Calificación”.

En este punto de la metodología se consolidan los conceptos más relevantes e importantes de su desarrollo, además de algunos pasos que se deben realizar antes de concluir con la generación de la matriz de riesgos de la información, para que de esta manera la entidad pueda realizar el tratamiento de los riegos teniendo la seguridad de establecer la mejor metodología que le permitirá ajustarse a las ordenanzas de gobierno nacional además de proteger su información y la de sus usuarios.

Diligenciamiento Matriz de Riesgos

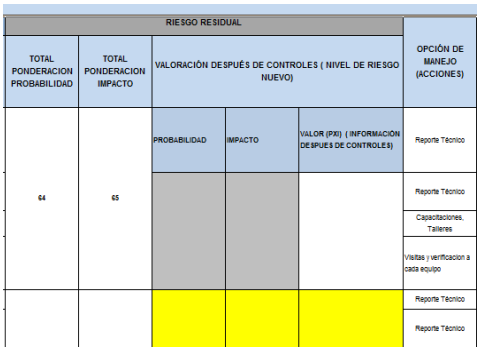
En las siguientes figuras se presenta la matriz de riesgos de información.



RIESGO INHERENTE			CRITERIOS ERCA (Evitar, Reducir, Compartir, Asumir)
PROBABILIDAD	IMPACTO	VALOR (PXI) (INFORMACIÓN ANTES DE CONTROLES)	
3	4	Extremo	REDUCIR EL RIESGO por medio de acciones de control preventivo y correctivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado.
			REDUCIR EL RIESGO por

Figura 13. Matriz de riesgos (parte a)

Fuente: Elaboración propia



RIESGO RESIDUAL					OPCIÓN DE MANEJO (ACCIONES)
TOTAL PONDERACION PROBABILIDAD	TOTAL PONDERACION IMPACTO	VALORACIÓN DESPUÉS DE CONTROLES (NIVEL DE RIESGO NUEVO)			
		PROBABILIDAD	IMPACTO	VALOR (PXI) (INFORMACIÓN DESPUES DE CONTROLES)	Reporte Técnico
64	65				Reporte Técnico
					Capacitaciones, Talleres
					Visitas y verificacion a cada equipo
					Reporte Técnico
					Reporte Técnico

Figura 14. Matriz de riesgos (parte b)

Fuente: Elaboración propia

El paso para seguir es el diligenciamiento de la matriz de riesgos:

- **Generalización Activo de Información (Contenedor):** en esta casilla se deben consignar los contenedores de los activos de información que se obtuvieron en la clasificación de activos de información.

- **Criticidad:** en esta casilla se diligencia la criticidad del activo en mención.

- **Identificador del riesgo:** en esta casilla se establece una nomenclatura en orden ascendente anteponiendo la letra R, de la cantidad de riesgos establecidos, ejemplo (R1, R2, R3……Rn).

- **Riesgo:** en esta casilla se definen los riesgos que los encargados de la seguridad de la información y el grupo interdisciplinar han definido, se pueden establecer la cantidad de riesgos que se consideren.

- **Causas:** en esta casilla se diligencian las causas identificadas, estas pueden ser internas o externas, según lo que se defina a través del contexto estratégico.

- **Efectos y/o Consecuencias:** en esta casilla se diligencian los efectos y/o consecuencias una vez materializado el riesgo, describir el impacto o impactos generados desde el punto de vista estratégico y de riesgos.

- **Riesgo Inherente:** Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que establezcan, tiene en cuenta la Probabilidad y su Impacto dando como resultado la criticidad del riesgo.

    - **Probabilidad:** Se debe observar la tabla determinación de la probabilidad del riesgo y elegir el nivel que se encuentra, apuntar su valor en esta casilla.

    - **Impacto:** Se debe observar la tabla determinación de la probabilidad del impacto y elegir el nivel que se encuentra, apuntar su valor en esta casilla.

    - **Criticidad del Riesgo (PxI):** La criticidad del riesgo es el producto de la probabilidad por el impacto, esta casilla define el estado que toma el riesgo dentro del mapa de calor, se establece posicionando la probabilidad en primer lugar, en segundo lugar se posiciona el Impacto, por citar un ejemplo: tenemos que la probabilidad de que ocurra el riesgo, tiene un valor de 4 corresponde a Probable y el impacto causado un valor de 5 corresponde a catastrófico, por tanto el producto es (4x5)= 20, en el mapa de calor estará posicionado en **E20 con color Rojo,** significa riesgo extremo traduciéndolo de la tabla valoración de riesgos.

De igual forma, se distribuyen los riesgos (inherentes y residuales) en las zonas de riesgo de acuerdo con el siguiente mapa de calor representado en la Tabla 16:

Probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Improbable (1)	B 1	B 2	M 3	A 4	A 5
Raro (2)	B 2	B 4	M 6	A 8	E 10
Posible (3)	B 3	M 6	A 9	E 12	E 15
Probable (4)	M 4	A 8	A 12	E 16	E 20
Casi Seguro (5)	A 5	A 10	E 15	E 20	E 25

Tabla 14. Mapa de calor

Fuente: Guía No 7 MINTIC

En la tabla 13, se representan las nomenclaturas que se expresan en el mapa de calor

B: Zona de Riesgo Baja: Asumir el Riesgo
M: Zona de Riesgo Moderada : Asumir Riesgo - Reducir Riesgo
A: Zona de Riesgo Alta: Reducir Riesgo - Evitar - Compartir o Transferir
E: Zona de Riesgo Extrema: Reducir el Riesgo - Evitar - Compartir o Transferir

Tabla 15. Nomenclatura de Zonas

Fuente: Elaboración propia

.

Valoración de los riesgos

Teniendo la probabilidad y la valoración del impacto de cada riesgo, se constituyen los niveles de riesgos (inherentes y residuales luego de aplicar los controles identificados) teniendo una clasificación propia como se puede apreciar en la siguiente tabla.

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo Extremo	**Mayor o igual a 10**	**Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad, reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa o compartir y/o transferir el riesgo.**
Riesgo Alto	**Mayor que 4 y menor a 12**	**Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado o compartir y/o transferir el riesgo.**
Riesgo Moderado	**Mayor que o igual a 3 y menor o igual 6**	**Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor o compartir el riesgo.**
Riesgo Bajo	**Menor o igual a 4**	**Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.**

Tabla 16. Tabla valoración de riesgos

Fuente: Guía No 7 MINTIC

- **Criterios ERCA:** Hace referencia al tratamiento que se le va a dar al riesgo, entre estos están: Evitar, Reducir, Compartir o Asumir, se debe escoger solo uno. Los criterios se pueden apreciar en la siguiente tabla.

Evitar	**Tomar las medidas encaminadas a prevenir su materialización.** **Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.**
Reducir	Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.
Compartir	Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del

	riesgo con otra entidad.
Asumir	Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, la cabeza principal de la organización simplemente acepta la perdida residual probable y elabora planes de contingencia para su manejo.

Tabla 17. Criterios ERCA

- **Controles:** hacen referencia a las acciones que se realizan para prevenir la materialización del riesgo, por lo tanto, permite definirlo como la preparación de prácticas con anticipación para un determinado fin, a prever un daño o a anticiparse a una dificultad, los encargados de la seguridad de la información en conjunto con el grupo interdisciplinar pueden diseñar los controles, sin embargo en la norma ISO 27002, se especifican algunos tipos de controles.

- **Tipo de Control:** en esta casilla se pueden escoger dos tipos de control, de probabilidad o de impacto, el primero hace referencia a disminuir la probabilidad de que ocurra un riesgo, el segundo hace referencia a disminuir el impacto o daño causado.

- **Evaluación de Riesgo Residual:** Después de evaluar el riesgo inherente y de definir cómo será tratado el riesgo a través de los controles, se realiza una evaluación preliminar del tratamiento, que evalúa cuánto del tratamiento reduce el riesgo. Esto le permite identificar los activos y procesos de la entidad que están expuestos a riesgos.

  Evaluar el riesgo residual implica especificar un porcentaje de tratamiento para definir cuánto del tratamiento reduce el riesgo inherente.

  El porcentaje de tratamiento se basa en una evaluación esperada de los esfuerzos de tratamiento establecidos, antes de que los controles se hayan probado para proporcionar aseguramiento.

  Los ítems propuestos para la evaluación de los controles y sus respectivos puntajes se proporcionan a continuación, sin embargo, esta metodología permite cambiar estos ítems y sus puntajes, agregar nuevos o eliminar existentes, según se considere necesario.

- Herramientas para ejercer control (5 puntos)

- Manuales, instructivos o procedimientos, capacitación (15 puntos)

- Efectividad del control (30 puntos)

- Responsables del control y seguimiento (5 puntos)

- El control es automático (20 puntos)
- El control es manual (10 puntos)
- Frecuencia de ejecución del control y seguimiento (15 puntos)
- Ponderación de controles: hace referencia a la suma de puntos de evaluación establecida a un control específico, el valor máximo estaría dado en 100 puntos.
- **Riesgo Residual:** Es aquel riesgo que subsiste, después de haber implementado controles, es aquél que permanece después de desarrollar respuestas a los riesgos, este refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones o controles para mitigar el riesgo inherente.
- Total de la ponderación de Probabilidad: en esta casilla se debe realizar el promedio de las calificaciones que se dieron a los controles del tipo probabilidad.
- Total de la ponderación de Impacto: en esta casilla se debe realizar el promedio de las calificaciones que se dieron a los controles del tipo impacto.
- **Valoración Después De Controles (Nivel De Riesgo Nuevo):** en esta casilla se deben establecer los nuevos valores de probabilidad e impacto y el nuevo valor de la criticidad del riesgo (PxI) de la siguiente manera:

Se deben tener presente el valor total de la ponderación de probabilidad y el total de la ponderación de impacto, ahora bien, se compara cada uno de ellos con la primera columna de la siguiente tabla de rangos de calificación de controles y según en el rango donde pertenezca, se deben disminuir la cantidad de cuadrantes que se indique 0, 1 o 2, esta disminución se realiza en el mapa de calor antes mencionado siempre partiendo de la posición inicial del riesgo Inherente (PxI - antes de controles), de esta manera se tendrá la nueva valoración del riesgo después de controles (PxI - después de controles).

En la Tabla 18 se ilustran los rangos de calificación y los cuadrantes a disminuir en probabilidad e impacto.

Rango de calificación de controles:

Rangos de calificación de los controles	Cuadrantes a disminuir en Probabilidad	Cuadrantes a disminuir en Impacto
entre 0 /50	0	0
entre 51/75	1	1
entre 76/100	2	2

Tabla 18. Rango de calificación de los controles

Fuente: Elaboración propia

- **Acciones:** Las acciones describen cómo se llevarán a cabo los controles, la organización, cronogramas, condiciones especiales que se definan.
- **Registro:** Los registros son todos los tipos de evidencias que se puedan generar de la implementación de los controles, estos pueden ser indicadores, informes, documentos, listas de chequeo, formatos especiales que la entidad requiera.
- **Responsable:** El responsable o responsables son los encargados del proceso de implementación de los controles y sus evidencias.
- **Fecha de terminación:** se debe apuntar la fecha de terminación de la implementación de controles.

SEGUIMIENTO

MONITOREO Y REVISIÓN / COMUNICACIÓN Y CONSULTA

La Entidad *"evaluará el desempeño de la implementación de la metodología para el levantamiento y gestión de riesgos de los activos de información"*, por medio de un monitoreo que permita hacer seguimiento de las gestiones que se están llevando a cabo y evaluar la eficiencia en su puesta en marcha, adelantando comprobaciones al menos una vez al semestre o cuando la entidad lo considere necesario, evidenciando y comunicando constantemente a la alta gerencia aquellas situaciones o causas que puedan estar influyendo en la aplicación de las acciones de tratamiento**.**

El monitoreo semestral o en el momento que se determine, debe estar a cargo de los responsables de la seguridad de la información de la entidad, aplicando y proponiendo los correctivos y ajustes que necesarios para emprender un efectivo manejo de los riesgos de Seguridad y Privacidad de la Información.

Se espera que esta metodología para el levantamiento y gestión de riesgos de los activos de información de las alcaldías categoría 6 del departamento de Boyacá, tomando como referencias las guías 5 y 7 del MinTIC, para el mejoramiento de los índices de seguridad digital de estas organizaciones, pueda ser usada en el Departamento de Boyacá y se replique a los demás departamentos como la mejor alternativa para la protección de la información del estado y de la ciudadanía con el fin de brindar mejores servicios de una manera segura y confiable.

CRONOGRAMA Y PRESUPUESTO

Actividad	mes 1	mes 2	mes 3	mes 4	mes 5	mes 6
Programación visitas a dependencias	X					
Capacitación a funcionarios y diligenciamiento Matriz Activos de Información	X	X				
Aplicación de listas de chequeo		X	X			
Levantamiento de Activos en la Entidad			X	X		
Análisis, verificación y clasificación de los Activos de información				X	X	
Análisis de Riesgos					X	X
Diligenciamiento de Matriz de Riesgos						X

Tabla 19. Cronograma. Fuente Elaboración propia

PRESUPUESTO:

El presupuesto está basado en el salario mínimo pagado por el empleador en una entidad del estado colombiano, sin embargo, dependiendo de la formación académica y experiencia del profesional este puede incrementar.

Salario mínimo mensual ejemplo pagado por empleador	
Concepto	**Valor**
Salario Mensual	$ 877,803
Subsidio de transporte	$ 102,854
Prima (1 salario anual + transporte)	$ 81,721
Cesantías (1 salario anual)	$ 81,721
Intereses sobre cesantías (12% cesantías año anterior)	$ 9,807
Aporte Seguridad Social - Salud (8.5%)	$ 74,613
Aporte Seguridad Social - Pensión (12%)	$ 105,336
Aporte Seguridad Social - ARL (Riesgo V - 6.96%)	$ 61,095
Parafiscales - Caja de compensación (4%)	$ 35,112
Parafiscales - ICBF (3%)	$ 26,334
Parafiscales - Sena (2%)	$ 17,556
Total pagado	**$ 1,473,953**

Tabla 20. Salario mínimo mensual ejemplo pagado por empleador. Fuente Elaboración propia

Asumiendo que el encargado del área informática de la Alcaldía se dedica exclusivamente a realizar las actividades propuestas durante los seis meses, el costo de la implementación será de **$8.843.718 pesos colombianos**.

CONCLUSIONES

- El modelo se seguridad y privacidad de la información proporcionado por el MINTIC, permite sensibilizar y sincronizar a todas las entidades del estado frente a las disposiciones gubernamentales encargadas de favorecer al incremento de la transparencia en la gestión pública, incentivando el uso de las mejores prácticas de seguridad de la Información como plataforma para la aplicación del concepto de seguridad digital.

- La propuesta metodológica desarrollada en este proyecto cuenta con las herramientas apropiadas para que las entidades que carecen de personal especializado en seguridad de la información, puedan implementar las guías 5 y 7 del MSPI, cumpliendo con los lineamientos del Gobierno y a su vez estar preparados para implementar el sistema de gestión de seguridad de la información.

- Todas las organizaciones deben contar políticas claras, enfocadas al tratamiento de la información, estas deben definir un sistema para la gestión de activos y un sistema de gestión de riesgo asegurando la protección de los activos de información y garantizando la continuidad del negocio.

- La implementación de un sistema de gestión de seguridad de la información requiere conocer el contexto organizacional de la entidad, esto se logra en compañía de un grupo interdisciplinar, esta metodología hace posible la creación e integración de este grupo en el desarrollo de la gestión del riesgo.

- Ésta metodología ha desarrollado un innovador sistema de clasificación de activos de información mediante contenedores, estos permiten realizar un análisis de riesgos ágil y eficiente además de incluir o excluir activos de información para la aplicación de controles.

- La metodología está diseñada especialmente para las alcaldías categoría 6 del departamento de Boyacá, sin embargo, se concluye que puede ser usada por demás entidades públicas y privadas que requieran implementar el desarrollo de las guías 5 y 7 del MINTIC.

TRABAJOS FUTUROS

- Se propone para trabajos futuros, la implementación de esta metodología en entidades que requieran empezar con un sistema de gestión y seguridad de la información.

- Se propone diseñar un aplicativo de software para el levantamiento de activos de información de la entidad de manera tal, que se pueda realizar recolección y consulta de forma más ágil y eficiente; que permita hacer seguimiento y actualización constante.

- Se propone sistematizar la matriz de riesgos de información de manera tal, que se el seguimiento y calificación de controles no se realice de forma manual.

- Se propone realizar las metodologías a las guías faltantes del Modelo de Seguridad y Privacidad de la Información MSPI.

REFERENCIAS

Abril, A., Jarol, P., & John, B. (2013). Risk Analysis in Security of Information. Risk Analysis in Security of Information. 39-53.

Alcaldía De Tunja, D. (2019). Decreto 0202. (13 de 06 de 2019).

Alexander, A. G. (2010). *Análisis Del Riesgo Y El Sistema De Gestion De Seguridad De La Información El Enfoque: Iso-27001-20050.* LIMA,PERÚ: Eficiencia Gerencial Y Productividad.

Andrade Serrano Hernán , Otero Dajud Emilio Ramón, V. (2009). Edición, diario Oficial; código penal, congreso de Colombia.

Antomás Osés, j. (2011). *Confidencialidad e historia clínica - Consideraciones ético-legales.* Pamplona: Complejo Hospitalario de Navarra.

Antomás, J., & del Barrio, H. (2011). *Confidencialidad e historia clínica. Consideraciones ético-legales Confidentiality and the medical record. Ethical-legal considerations.*

Antonio Dussan Clavijo Palabras clave, C. (2006). *Políticas de seguridad informática.*

Burgos Salazar, J., & Campos, P. (s.f.). *Modelo Para Seguridad de la Información en TIC.* Universidad del Bio - Bio, Chile.

Cano, J. (2004). *Inseguridad informática: Un concepto dual en seguridad informática.*

Cano, J., & Segurinfo, C. (2008). Seguridad Informática en Colombia Tendencias 2008 1.

Cortés R., D. M., & Ardila, A. (2012). Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001. Universidad EAN.

Cortés R., D. M., & Ardila, A. V. (2012). *Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001. .* Bogotá: Universidad EAN.

Edición, diario Oficial; codigo penal, CONGRESO DE COLOMBIA; Andrade Serrano Hernán , Otero Dajud Emilio Ramón, Varón Cotrino Germán, R. (2009). Ley 1273 de 2009 atentados contra la confidencialidad. *VII*, 30.

Ferrer Ballestrer, M. A. (2006). *Autenticación De Personas A Partir De La Biometría De La Región Dígito Palmar.* España: Universidad de Las Palmas de Gran Canaria.

Francisco, A. (2013). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN LA OFICINA DE SISTEMAS DE INFORMACIÓN Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE CÓRDOBA. *Journal of Chemical Information and Modeling, 53*(9), 1689-1699.

Función Pública, D. (2012). Decreto 2482. (03 de 12 de 2012).

Furag. (2019). *Furag 2019*. Obtenido de https://www.funcionpublica.gov.co/web/mipg/resultados-2018

Gómez, R., Hernán Pérez, D., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información Methodology and Governance of the IT Risk Management. 109-118.

Gonzalez Hernandez, M. (2014). Actualidad De Colombia En Seguridad De La Información. Bogotá DC: Repositorio Unipiloto.

Huillica, M., & Monzón, A. (2015). Pontificia Universidad Católica. *Propuesta Pucp*.

Irigoyen, P., Lima -Perδ, M., & Alexander, A. (2010). *Eficiencia Gerencial y Productividad S. A. Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El Enfoque ISO 27001:2005 Por.* Perú.

Jian, Z., Li, J., Ferrer Ballester, M., Bernardino, J., Hernández, A., Travieso González, C., y otros. (2006). Autenticación De Personas A Partir De La Biometría De La Región Dígito Palmar. España: Universidad de Las Palmas de Gran Canaria.

Ley 489. (19 de 12 de 1998). (1998). Ley 489. (19 de 12 de 1998).

Manuel Santos Calderón, J., Lorena Gutiérrez Botero Ministra de la Presidencia Juan Fernando Cristo Bustos, M., Cárdenas Santamaría Ministro de Hacienda Crédito Público Yesid Reyes Alvarado, M., Carlos Villegas Echeverri Ministro de Defensa Nacional Aurelio Iragorri Valencia, L., Gaviria Uribe, A., Eduardo Garzón Ministro de Trabajo María Lorena Gutiérrez Botero, L., y otros. (2016). *CONPES 3854, Consejo Nacional de Política Económica y Social.*

Mayorga Delgado, A. (2014). Lineamientos, Tendencias Y Estrategias Sobre Ciberseguridad Y Ciberdefensa En Colombia. Bogotá: Repositorio Unipiloto.

Mesquida, A. L., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. *REICIS, Revista Española de Innovación*, 28-29.

Mesquida, A., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001. *REICIS, 6*(3), 24-35.

MinTIC. (2015). Decreto 1078.

MinTIC. (2019). Fortalecimiento de la Gestión TI en el Estado. Bogotá.

MinTIC Ley 1341, (. d. (2009). *Ley 1341. (29 de 07 de 2009).* MinTIC.

MinTIC, D. (2014). Decreto 2573. (12 de 12 de 2014).

MinTIC, D. (2018). *Decreto 1008. (14 de 06 de 2018).*

MinTIC, L. (2009). *Ley 1341. (29 de 07 de 2009).* MinTIC.

Montaño Orrego, V. (2011). *La gestión en la seguridad de la información según Cobit, Itil e Iso 27000.*

Montaño Orrego, V. (2011). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano*, 21-23.

NIEVES, A. (2017). DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA ISO/IEC 27001:2013.

Norma ISO 27001. (2013). Normas ISO 27001.

NORMA ISO 27001. (10 de 09 de 2013). *NORMAS ISO 27001.* Obtenido de https://www.normas-iso.com/iso-27001/

Ochoa Arévalo, P. (2015). Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. *Revista Tecnológica ESPOL-RTE, 28*(3), 1-17.

Ojeda-Pérez, J. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia.* Bogotá, Colombia.

Roberto Hernandez Sampieri, Carlos Fernandez Collado, & Pilar Baptista Lucio. (s.f.). *Metodología de la Investigación.*

Rodrigo, B. (2014). Implementación efectiva de un SGSI ISO 27001. *2014*, 30.

Romero Castro, M. I. (2018). *Introducción a la Seguridad Informatica y el Analisis de Vulnerabilidades.* Ecuador: 3 Ciencias.

Romero, M., Grace, C., Figueroa, L., Denisse, M., Vera, S., José, N., y otros. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades.* Ecuador.

Salazar, J., & Campos, P. (2009). Modelo para seguridad de la información en TIC. *CEUR*

Workshop Proceedings, 488, 234-253.

Seclén Arana, J., & Seclén Arana, J. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. *Repositorio de Tesis - UNMSM*.

Sierra Cubides, M., & Hurtado Castrillon, J. (2018). Modelo De Seguridad Y Privacidad De La Información Para La Alcaldía De Puerto Asís En Su Fase De Diagnostico Y Planificación. Bogotá.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes Aplicaciones y Estándares Segunda Edición.* Madrid: Pearson Educacion S.A.

Stallings, W. (2004). *Fundamentos de seguridad en redes: Aplicaciones y estándares, 2da Edición.* Madrid.

Stevanovi, B. (2011). Maturity Models in Information Security. *International Journal of Information and Communication Technology Research, 1*(2), 44-47.

Valencia-Duque, F., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*(22), 73-88.

ANEXOS

ANEXO 1.

Seguridad de la información

Lista de chequeo "Nombre de la Entidad"				**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"				
ITEM A EVALUAR		Seguridad de la información		
Objetivo		Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos organizacionales y leyes y regulaciones relevantes.		
	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Existen políticas para la seguridad de la información?				
¿Existen políticas de seguridad para el control y manejo de dispositivos móviles?				
¿Se clasifica la información de acuerdo por confidencialidad y grado crítico para la organización?				
¿Se tiene un esquema de clasificación de la información adoptado por la organización?				
¿Existen políticas para el control de acceso de usuarios a la información?				
¿Se cuenta con políticas para el uso de controles criptográficos?				
¿Se tienen implementadas políticas de restricción de software no autorizado?				
¿Se cuentan con políticas y procedimientos de transferencia de información?				
¿Existen políticas que garanticen la protección de datos personales?				
¿Se hacen revisiones y monitoreos periódicos, de las políticas para la seguridad de la información de la organización?				
¿Se tiene establecido separación de deberes (segregación de funciones), que se llevan a cabo dentro de la organización?				
¿Existen políticas de seguridad de la información para la gestión de proyectos?				
TOTAL CALIFICACIÓN				

ANEXO 2.

Gestión de activos

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Gestión de activos	
Objetivo		Lograr y mantener la protección apropiada de los activos organizacionales.	

	Cuestionario				
PREGUNTAS		**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Existe inventario de activos informáticos de la organización?					
¿Existe una revisión establecida sobre la propiedad de los activos?					
¿Se identifican, documentan e implementan reglas para el uso aceptable de los activos?					
¿Se lleva un control para la devolución de activos?					
¿Existe un control de transferencia para medios físicos?					
¿Se tiene un registro de disposición de medios físicos?					
TOTAL CALIFICACIÓN					

ANEXO 3.

Seguridad de los recursos humanos

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Seguridad de los recursos humanos	
Objetivo		Asegurar que los empleados, entiendan sus responsabilidades y sean adecuados para los roles que se les considera; reducir el riesgo de robo, fraude o mal uso de los medios.	

	Cuestionario				
PREGUNTAS		**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Se llevan a cabo procesos para el reclutamiento y selección del personal?					
¿Se llevan a cabo chequeos de verificación de antecedentes de todos los candidatos empleados?					
¿En el contrato se especifican los términos y condiciones del empleo?					
¿Se tiene un documento formal sobre las responsabilidades por parte de la dirección?					
¿Se llevan a cabo socializaciones para tomar conciencia, educación y formación en la seguridad de la información?					
¿Existen procesos disciplinarios para los miembros de la organización?					
¿Se lleva a cabo un proceso formal para la terminación o cambios de responsabilidades del empleado?					
¿Existe un proceso formal para que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de información y reducir los riesgos de error humano?					
¿Se tiene un control de devolución de activos por parte de los empleados al momento de la terminación del contrato laboral?					
¿Existe un procedimiento para revocación de permisos y derechos de acceso a los empleados al momento de la terminación del contrato laboral?					
TOTAL CALIFICACIÓN					

ANEXO 4.

Seguridad física y ambiental

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Seguridad física y ambiental	
Objetivo		Evitar el acceso físico no autorizado, daño e interferencia al área de sistemas y la información de la organización.	

	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Se tiene un control para la utilización de perímetro de seguridad (barreras tales como: paredes y puertas de ingreso controlado) para proteger áreas que contienen información y medios de procesamiento de información?				
¿Se implementan controles para diseñar y aplicar seguridad física en oficinas y medios de la organización?				
¿Se tienen controles para diseñar y aplicar protección física, contra daño por fuego, inundación, terremotos, explosión, disturbios civiles y otras formas de desastre natural o creados por el hombre?				
¿Existe personal de vigilancia constante dentro de la organización?				
¿Se ha instruido al personal de vigilancia sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?				
¿El centro de cómputo tiene salida al exterior?				
¿El espacio de distribución entre racks cuentan con la debida separación y por ende puntos de flexibilidad que permitan mantenimiento preventivo y correctivo?				
¿Los Racks cuentan con suministro de aire distribuido de forma proporcional al interior de los dispositivos?				
¿Existe un modelo que describa la construcción del centro de cómputo, proporcionando planos del mismo?				
¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?				

¿Existe alarma para detectar fuego (calor o humo) en forma automática??				
¿Existen extintores de fuego?				
TOTAL CALIFICACIÓN				

ANEXO 5.

Seguridad en la infraestructura

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Seguridad en la infraestructura	
Objetivo		Verificar el conocimiento que se tiene en la infraestructura del centro de datos y los sistemas de control establecidos.	

Cuestionario				
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Se tiene iluminación exterior del centro de datos, además de señalización del entorno que identifique la relación de los riesgos?				
¿Se tienen identificados los riesgos ambiéntales en el centro de datos y la distancia de los servicios de emergencia?				
¿Se tiene autenticación física de acceso a los dispositivos con apropiado uso y trabajo?				
¿Se tiene la documentación acerca de las rondas de guardia del edificio y las funciones del personal de seguridad?				
¿La calefacción y los sistemas de aire acondicionado mantienen la temperatura constante en el centro de datos?				
¿Las emisiones de radio afecten o hacen ruido en los sistemas electrónicos de cómputo al transmitir información?				
¿Existe protección polo a tierra?				
¿Las condiciones de energía pueden prevenir una pérdida de datos?				
¿Los sistemas de reserva eléctrica proveen la continuidad del flujo eléctrico durante un apagón o reducción de energía?				
¿Se tienen generadores eléctricos que garanticen la continuidad de trabajo de la organización?				
TOTAL CALIFICACIÓN				

ANEXO 6.

Seguridad de equipos

Lista de chequeo "Nombre de la Entidad"				**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"				
ITEM A EVALUAR		Seguridad de equipos		
Objetivo		Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.		
	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Los equipos están ubicados y protegidos de tal manera que se reduzcan riesgos, amenazas y peligros ambientales?				
¿Los equipos son protegidos contra fallos de energía y otras interrupciones causadas por fallos en los servicios públicos?				
¿El cableado de energía y de transmisión de información que llevan datos o sostienen los servicios de información está protegidos de la intercepción o daño?				
¿Existe un proceso para el mantenimiento periódico de equipos y así garantizar su continua disponibilidad e integridad?				
¿Se lleva un control de equipos, información y software para garantizar que no sean sacados de la organización sin autorización?				
¿Se llevan a cabo chequeos periódicos de monitoreo de datos confidenciales y software licenciado antes de su eliminación?				
¿El ingreso de los usuarios a los equipos se lleva a cabo por medio de un Login?				
¿Los equipos cuentan con un antivirus licenciado?				
¿El sistema operativo de los equipos cumple con las necesidades de la organización?				
¿Los archivos y carpetas que contengan información crítica están protegidos contra intrusos?				
TOTAL CALIFICACIÓN				

ANEXO 7.

Gestión de las comunicaciones y operaciones

Lista de chequeo "Nombre de la Entidad"				**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"				
ITEM A EVALUAR		Gestión de las comunicaciones y operaciones		
Objetivo		Asegurar la operación correcta y segura de os medios de procesamiento de la información.		
	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Se tienen documentados los procedimientos de operaciones y se tienen dispuestos a los usuarios que los necesiten?				
¿Se lleva a cabo un control de cambios en los medios y sistemas de procesamiento de la información?				
¿Se tiene un control para segregar deberes y áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o mal uso de los activos de la información				
? ¿Se tiene un control para separar los medios de desarrollo, pruebas y operaciones para reducir los riesgos de acceso no-autorizados o cambios en el sistema de operación?				
TOTAL CALIFICACIÓN				

ANEXO 8.

Planeación y aceptación del sistema.

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Planeación y aceptación del sistema.	
Objetivo		Minimizar el riesgo de fallas en los sistemas.	

	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Existe un plan de gestión de capacidad del sistema en la organización?				
¿Se monitorean, afinan y realizan proyecciones del uso de los recursos para asegurar el desempeño de los sistemas de información?				
¿Se llevan a cabo pruebas de aceptación del sistema?				
¿Se establecen criterios para los sistemas de información, actualizaciones y versiones nuevas de los sistemas durante su desarrollo y antes de su aceptación?				
TOTAL CALIFICACIÓN				

ANEXO 9.

Protección contra software malicioso

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Protección contra software malicioso	
Objetivo		Proteger la integridad del software y la información de la organización.	

	Cuestionario				
PREGUNTAS		**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Existe un control para la prevención de software malicioso?					
¿Se llevan a cabo controles de detección, prevención y recuperación para protegerse de códigos maliciosos?					
¿Se hace un proceso de sensibilización a los empleados, sobre la instalación del nuevo software?					
¿Se tiene un manual de buenas prácticas para el control de malware?					
¿Se tiene establecido de respuesta ante la infección por ejecución de malware?					
¿Se tienen implementadas herramientas que faciliten la detección de malware?					
¿Se llevan a cabo actualizaciones periódicas de las herramientas de detección de malware?					
¿Se tienen implementadas medidas y controles contra software malicioso?					
TOTAL CALIFICACIÓN					

ANEXO 10.

Gestión de seguridad de redes

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Gestión de seguridad de redes	
Objetivo		Asegurar la protección de la información de redes y la protección de la infraestructura de soporte.	

Cuestionario

PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Se tiene un proceso de Respaldo (Back -up) para mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones?				
¿Se lleva a cabo testeos periódicos de la red?				
¿Se tiene control de la red que garantice el uso adecuado de la misma y así poderla proteger de posibles amenazas?				
¿Existe un plan de contingencia contra fallos de los servicios de red?				
¿Se identifican los dispositivos de seguridad, niveles de servicio y requerimientos incluidos en cualquier contrato de servicio de red?				
¿Los enlaces de la red se testean frecuentemente?				
¿Todos los nodos se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?				
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?				
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros establecido en (TIA/EIA 568-C, ISO 11801, EN50173)?				
¿Cuentan con conmutadores en red, para la expansión de redes locales?				
¿Las direcciones IP´S de los equipos de cómputo son implementadas de forma fija				
¿La red cuenta con los equipos y aplicaciones (protección)				

necesarias para tener un mayor resguardo de intrusos activos (hackers)?				
TOTAL CALIFICACIÓN				

ANEXO 11.

Intercambio de información

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Intercambio de información	
Objetivo		Mantener la seguridad de la información y software intercambiados dentro de la organización y con cualquier entidad externa.	

	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Existen controles para proteger el intercambio formal de información a través de todos los medios de comunicación?				
¿Existen acuerdos para el intercambio de información y software entre la organización y entidades externas?				
¿Se tienen controles sobre los medios que contienen información a personal no autorizado?				
¿Existen controles para proteger adecuadamente los mensajes electrónicos?				
¿Se desarrollan e implementan políticas y procedimientos para proteger la información asociada con la interconexión de sistemas e información organizacional?				
¿Se protege la información involucrada en comercio electrónico transmitida a través de redes públicos?				
¿Existe control para la protección de información involucrada con transacciones en línea para evitar las transmisiones incompletas, rutas equivocadas o alteraciones no autorizadas?				
TOTAL CALIFICACIÓN				

ANEXO 12.

Monitoreo

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Monitoreo	
Objetivo		Detectar actividades de procesamiento de información no autorizada.	

	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Se tiene registro de actividades de auditoria realizadas a la organización?				
¿Existen procedimientos para monitorear el uso de medios de procesamientos de información?				
¿Se tienen controles para proteger los medios de registro y la información de registro contra alteraciones y accesos no autorizados?				
¿Se lleva un registro de las actividades del administrador y operadores del sistema?				
¿Se registran las fallas, se analizan y se toma una acción apropiada sobre ellas?				
TOTAL CALIFICACIÓN				

ANEXO 13.

Control de acceso

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Control de acceso	
Objetivo		Controlar acceso a la información	

Cuestionario				
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Se definen los roles de usuarios y de grupos en función del tipo de información al que podrán acceder?				
¿Asignan los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso?				
¿Definen y aplican un procedimiento para dar de alta/baja o modificar las cuentas de usuario?				
¿Se determinan e implantan las técnicas de autenticación más apropiados para permitir el acceso a la información de la organización?				
¿Se establecen los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la organización?				
¿Se revisa cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados?				
¿Se desactivan los permisos de acceso y eliminan las cuentas de usuario una vez finalizada las relaciones laborales?				
TOTAL CALIFICACIÓN				

ANEXO 14.

Responsabilidades del usuario

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Responsabilidades del usuario	
Objetivo		Evitar el acceso de usuarios no autorizados y el compromiso o robo de la información y los medios de procesamiento de la información.	

Cuestionario				
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Los usuarios acceden al sistema por medio de usuario y contraseña?				
¿Se requiere a los usuarios seguir buenas prácticas en la selección y uso de las claves?				
¿Se requiere que los usuarios se aseguren de dar la protección apropiada al equipo destinado?				
¿Existen políticas de pantalla y escritorio limpio para los documentos y medios de almacenamientos removibles?				
TOTAL CALIFICACIÓN				

ANEXO 15.

Control de acceso a redes

Lista de chequeo "Nombre de la Entidad"			**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"			
ITEM A EVALUAR		Control de acceso a redes	
Objetivo		Evitar el acceso no autorizado a los servicios de red.	

	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Existe una política sobre el uso de los servicios de red?				
¿Se lleva a cabo un control de autenticación del usuario para conexiones externas?				
¿Se tienen procesos de identificación de equipos en la red?				
¿Se cuenta con un modelo de protección del puerto de diagnóstico remoto?				
¿Existe política de segregación de red de los servicios de información, usuarios y sistemas de información?				
¿Se tienen controles de restricción de la capacidad de conexión de usuarios en redes compartidas?				
¿Se tiene implementados controles 'routing' para las redes, asegurando las conexiones de cómputo y los flujos de información?				
TOTAL CALIFICACIÓN				

ANEXO 16.

Seguridad en los procesos de desarrollo y soporte

Lista de chequeo "Nombre de la Entidad"				**Fecha:** DD/MM/AA
Nombre Responsable: "Nombre del encuestador"				
ITEM A EVALUAR		Seguridad en los procesos de desarrollo y soporte		
Objetivo		Mantener la seguridad del software e información del sistema de aplicación		
	Cuestionario			
PREGUNTAS	**SI**	**NO**	**N/A**	**PORCENTAJE %**
¿Se tienen implementados controles mediante el uso de procedimientos formales de control de cambios?				
¿Cuándo se cambian los sistemas operativos, revisan y prueban aplicaciones críticas de la organización para asegurar que no exista un impacto adverso en las operaciones o seguridad?				
¿Se tienen controles para limitar los cambios necesarios y que estos sean administrados estrictamente?				
¿Se tienen controles para evitar la filtración de la Información?				
¿El desarrollo del software es monitoreado y supervisado por la organización?				
¿Se tienen controles para obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información?				
TOTAL CALIFICACIÓN				

ANEXO 17.

Anexo_17_Matriz Levantamiento Activos De Información

Lugar de consulta:

https://1drv.ms/x/s!ArPHYU5d70VvjjmdmANdKtIRxXfU?e=zG9ddv

ANEXO 18.

Anexo_18_Matriz De Riesgos De La Información

Lugar de consulta:

https://1drv.ms/x/s!ArPHYU5d70Vvjjsy9h7igG05Cg-H?e=M6JoNQ

https://1drv.ms/x/s!ArPHYU5d70Vvjjz_F-uwMAbaMlLH?e=61ETeh

ANEXO 19.

Anexo_ 19_Diagrama Flujo Procedimiento

Lugar de consulta:

https://1drv.ms/b/s!ArPHYU5d70Vvjjjgfejs5gpabTZ0?e=ROagUB

ANEXO 20.

Anexo_20_Controles_Iso27002-2013

Lugar de consulta:

https://1drv.ms/b/s!ArPHYU5d70VvjjfKi6ZSVvcZ6lzR?e=bkxG6L

ANEXO 21.

Anexo_21_Matriz Clasificación de Activos

Lugar de Consulta:

https://1drv.ms/x/s!ArPHYU5d70Vvjjpr7NNCsBqSa_Av?e=IeegTz