UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD PARA EL CONTROL DE LA INFORMACIÓN DEL ÁREA DE TICS DE LA EMPRESA FLOWER VILLAGE ECUADOR BASADA EN LA NORMA ISO 27002"

Realizado por:

Ing. Diego Augusto Bonilla Montenegro

Director del proyecto:

Msc. Estrella Mogollón Walter Edison

Como requisito para la obtención del título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD EN REDES Y COMUNICACIÓN

DECLARATORIA

El presente trabajo de investigación titulado:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD PARA EL CONTROL DE LA INFORMACIÓN DEL ÁREA DE TICS DE LA EMPRESA FLOWER VILLAGE ECUADOR BASADA EN LA NORMA ISO 27002"

Realizado por:

DIEGO AUGUSTO BONILLA MONTENEGRO

Como requisito para la Obtención del Título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA

Ha sido dirigido por el profesor

Msc. Estrella Mogollón Walter Edison

Quien considera que constituye un trabajo original de su autor

_____

Msc. Estrella Mogollón Walter Edison

DIRECTOR

LOS PROFESORES INFORMANTES

Los Profesores Informantes:

ING. RODRÍGUEZ ARBOLEDA VERÓNICA ELIZABETH, MBA

ING. PAZMIÑO FLORES CHRISTIAN DAVID, MSC

Después de revisar el trabajo presentado,

lo han calificado como apto para su defensa oral ante

el tribunal examinador

Verónica Elizabeth Rodríguez Arboleda	Christian David Pazmiño Flores

Quito, 11 de junio de 2018

DEDICATORIA

Los desafíos y logros que alcanzamos, tienden a ser mayores conforme avanza nuestra vida, algunos más importantes que otros, pero sin duda todos conllevan un grado de esfuerzo; este proyecto que inicio como una idea y que ahora concluye, se la dedico a mis padres, que a pesar de todo siempre han estado conmigo alentándome a que supere mis propios límites, a mi esposa quien con su consejos y amor me acompaña cada día de mi vida y a mis compañeros de maestría con quienes comporta una gran amistad.

AGRADECIMIENTOS

A Dios,

A mis padres, por ser quienes me inculcaron valores y respeto por el trabajo,

A mi esposa Mariela, por amarme y apoyarme en todo momento,

Al Ing. Edison Estrella, por guiarme en todo este proceso para ser mejor profesional,

A mis compañeros Marco, Bryan, David, Wilson; por la aventura que iniciamos, de la cual todos ganamos experiencia y los más importante una gran amistad.

RESUMEN

Las flores por su belleza y calidad constituyen una de las principales cartas de presentación para el Ecuador, para la empresa Flower Village el cumplimiento de estándares para la exportación no solo está ligado a la calidad de su producto, sino también a cumplir con las exigencias de la Alianza Empresarial para el Comercio Seguro BASC, la cual busca establecer medidas que prevengan el tráfico de drogas a través de las exportaciones, con el uso de normas para la seguridad de la información y protecciones para el comercio internacional.

Esta investigación tiene como objetivo fundamental diseñar una Política de Seguridad para el Control del la Información en base a la norma ISO 27002, la misma que proporcione lineamientos básicos para la gestión de la información en el servicio de storage, que es administrador por el área de TICS.

Se presentará un análisis del por qué usar la norma 27002 dentro del Capítulo I, el Capítulo II en cambio propone un análisis y diseño, con el uso de la información e identificación de los riesgos, por último, el Capítulo III presenta una propuesta usando la norma ISO 27002 y los controles seleccionados, todo esto con el fin de que la información dentro del servicio de storage, conserve integridad y disponibilidad.

ABSTRACT

The flowers for their beauty and quality constitute one of the main letters of presentation for Ecuador, for the Flower Village company, compliance with export standards is not only linked to the quality of its product, but also to meet the demands of the Business Alliance for Safe Trade BASC, which seeks to establish measures to prevent drug trafficking through exports, with the use of standards for information security and protections for international trade.

The main objective of this research is to design a Security Policy for the Control of Information based on the 27002 standard, which provides basic guidelines for the management of information in the storage service, which is managed by the TICS.

An analysis of why use rule 27002 will be presented within Chapter I, Chapter II instead proposes an analysis and design, with the use of information and identification of risks, finally, Chapter III presents a proposal using the ISO 27002 standard and the selected controls, all this in order that the information within the storage service, preserve integrity and availability.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

CAPÍTULO I

INTRODUCCIÓN

1.1 El problema de la investigación

En las últimas décadas, el avance de las tecnologías de la información, tanto en hardware software, han generado un crecimiento sin precedentes en la administración, seguridad, integridad de datos e infraestructura, pero de igual manera han surgido vulnerabilidades, producto de dichos avances contrastados con la falta de conocimientos y experiencia dentro de las organizaciones que adoptan estas tecnologías como elementos esenciales para su desarrollo.

Según Velásquez (Velásquez, 2015)

> La brecha existente entre la tecnología y la manera como se realiza de manera segura las operaciones al interior de la organización para garantizar la confidencialidad, disponibilidad e integridad de esa información que pasa, en la mayoría de los casos, por manos de uno, dos o más empleados sin tomar las medidas adecuadas para su correcto tratamiento. (p. 19)

La empresa **Flower Village Ecuador** intenta cambiar este panorama, mejorando la seguridad y confianza en el uso de la información.

1.1.1 Planteamiento del Problema

1.1.1.1 Diagnóstico

Flower Village Ecuador en su área de TICS, consolida información para exportar su producto a nivel mundial, en los últimos 6 meses la empresa ha generado altos ingresos por lo cual la empresa se está expandiendo rápidamente.

El área de TICS la gestión de la información en su servicio de storage se realiza sin una documentación que sustente los cambios o actualizaciones que se realiza, el día 9 de Noviembre del 2017, se realizó una reunión con el Ing. Marcelo Cárdenas quien esta temporalmente a cargo, en la misma expreso que el personal que labora en esta área desconoce cómo llevar un control de la información, posteriormente se realizó una inspección de campo, donde se pudo verificar

lo expuesto en la reunión, se pudo determinar que esto genera vulnerabilidades (en la administración, seguridad, integridad y redundancia de la información) en su servicio de storage.

Causa	Síntoma
El personal que labora en el área de TICS no gestiona correctamente información, desconoce cómo llevar un control de la información en su servicio de storage	• No hay parámetros para la gestión de la información • No se puede evidenciar que la información almacenada sea la correcta • La vigencia y validez de la información, no está garantizada

Figura 1. Causas y efectos del problema de la investigación
Fuente: Autor de la Investigación

Por lo antes expuesto se determina que el problema a resolver es, la falta de gestión de la información lo cual genera vulnerabilidades (en la administración, seguridad, integridad y redundancia de la misma) en su servicio de storage.

1.1.1.2 Pronóstico

Si Flower Village Ecuador en su área de TICS continúa gestionando la información sin parámetros de control y falta de conocimiento por parte del personal, los riesgos en sus servicios de almacenamiento van a crecer exponencialmente en mediada que la información se incremente, perjudicando la continuidad del negocio.

1.1.1.3 Control del Pronóstico

Para gestionar la información dentro de su servicio de almacenamiento, el área de TICS de la empresa Flower Village Ecuador, necesita generar documentación y con el uso de la norma ISO 27002; diseñar de una política de seguridad, para analizar los procesos y mejorar su eficiencia.

1.1.2 Formulación del Problema

La falta de gestión de la información por parte del personal del área de TICS de la empresa Flower Village Ecuador dificulta la identificación de vulnerabilidades para el control de la información en su servicio de storage.

1.1.3 Objetivo general

Diseñar una política de seguridad que permita el acceso, control y actualización de la información en el área de TICS de la empresa Flower Village Ecuador, en base a la norma ISO 27002, para la identificación de vulnerabilidades en el control de la información.

1.1.4 Objetivos específicos

- Identificar los problemas del área de TICS de la empresa Flower Village Ecuador mediante el uso de herramientas de investigación como observación, entrevistas y encuestas para determinar el estado actual.
- Realizar el levantamiento de la información mediante el uso de una metodología para conocer la vulnerabilidad en el área de TICS de la empresa Flower Village Ecuador.
- Analizar las vulnerabilidades en la gestión de la información, para seleccionar los dominios y controles que provee la Norma ISO 27002
- Diseñar la política de seguridad, con la cual se promuevan las mejores prácticas y la concientización en los usuarios en el manejo de la información.

1.1.5 Justificación

Para mejorar la gestión de la información en el servicio de almacenamiento (storage), el personal del Área de TICS de la empresa Flower Village Ecuador, pretende usar la norma ISO 27002; porque está orientada a la seguridad de la información, esta norma no exige utilizar todos los controles, más bien solo aquellos que sean necesarios, hay que puntualizar que no son simplemente buenas prácticas y que todo el diseño que se propone en este estudio posteriormente puede ser certificable.

Justificación Técnica

Flower Village Ecuador al ser una empresa exportadora debe cumplir con la certificación de la Alianza Empresarial para el Comercio Seguro BASC (2017) **“la cual busca establecer medidas que prevengan el tráfico de drogas a través de las exportaciones, con el uso de normas para la seguridad de la información y protecciones para el comercio internacional.”**

Justificación Metodológica

La presente investigación usa la metodología ISO 27002, con el fin de analizar e identificar riesgos, para posteriormente y manteniendo las mejores prácticas; diseñar una política de seguridad, con la cual se pretende alcanzar la certificación que solicita la Alianza Empresarial para el Comercio Seguro BASC.

La gestión de la información, en el servicio de storage; se maneja tanto de forma interna como externa, por lo cual la BASC solicita que está tenga protección, disponibilidad e integridad, con el uso de la norma ISO 27002 se puede establecer controles, para mejorar los procesos, sin afectar el funcionamiento y los objetivos de la empresa.

Con los antecedentes explicados anteriormente el diseño de una policita de seguridad es necesaria, no solo para el servicio de storage, sino como punto de partida para mejorar los distintos procesos que se manejan dentro del área de TICS de la empresa Flower Village Ecuador.

1.2 Marco Teórico

Flower Village Ecuador

Es una Empresa florícola que está ubicada en la provincia de Pichincha, constituida hace 18 años, posee una superficie de 52 hectáreas distribuidas en distintas fincas (Flower Village Matriz, Agroplantas, San Enrique, Flor Machachi y Flower Village Lasso), su producto es netamente de exportación a países como Estados Unidos, Rusia, Canadá, Holanda, Australia, etc. Su misión y visión es expuesta según Villegas Arciniegas (2017) en su documento Examen de Auditoría Integral al área de Recursos Humanos de la Empresa Flower Village Cia. Ltda.:

Misión: La producción y la exportación de rosas de diferentes colores y variedades recién cortadas, libres de plagas, insectos o enfermedades, así como con un follaje limpio y brillante, que - por su alta calidad - excede las necesidades de nuestros clientes. (p. 7)

Visión: Mantener una posición consolidada en el mercado floricultor, logrando ser el grupo más importante exportadores de flores a nivel internacional del país, comprometidos con la alta calidad de los productos, el cuidado del medio ambiente, con la seguridad y salud ocupacional de cada uno de nuestros colaboradores. (p. 7)

Norma ISO 27002

"Esta norma es muy relevante dentro del sector ya que, toma como base todos los riesgos a los que se enfrenta la organización en su día a día, tiene como objetivo principal establecer, implantar, mantener y mejorar de forma continua la seguridad de la información de la organización." (Sistemas de Gestión de Seguridad de la Información SGSI, 2016)

Figura 2. Características indispensables que debe poseer la información
Fuente: (Montoya, 2009)

El Estándar Internacional ISO/IEC 27002, se divide en 11 dominios; según Alvarado Peñaranda (2015) quien las resume:

1) **Políticas de Seguridad,** comprende tanto la elaboración del documento que recopile todas las políticas, como su revisión
2) **Organización de la Seguridad de la Información,** esta sección tiene dos objetivos de control que corresponden a la organización interna de la información y su trato con terceros
3) **Gestión de Activos,** posee dos activos que tratan la responsabilidad sobre activos, es decir, quién es responsable de qué activo, la clasificación de la información y su posterior manipulación
4) **Seguridad de los Recursos Humanos,** comprende todos los controles que se deben implementar para evitar la fuga de información por parte del personal de la empresa
5) **Seguridad física y del entorno,** este dominio comprende los controles necesarios tanto para la preparación de áreas seguras, como para el emplazamiento y protección de equipos

6) **Gestión de Comunicaciones y Operaciones,** este dominio es el más largo de toda la norma y comprende diez objetivos de control que aseguran una comunicación efectiva entre los sistemas de información
7) **Control de Acceso,** es lógico pensar que, en una empresa, no todos los usuarios deben tener acceso a toda la información de la empresa, sino que cada usuario debe acceder únicamente a la información con la que trabaja
8) **Adquisición, desarrollo y mantenimiento de sistemas de información,** para que la información de una empresa esté debidamente resguardada, es necesario que el sistema de seguridad que se ha implementado esté en una continua revisión
9) **Gestión de Incidentes en la seguridad,** al implementar un sistema de gestión de la Seguridad de la Información, cualquier incidente implica un fallo en el mismo y ha de ser controlado correctamente para que no afecte otras áreas de la organización
10) **Gestión de la continuidad del negocio,** este dominio tiene un solo objetivo y consiste en el alineamiento de los objetivos del SGSI[1] con los objetivos de la compañía
11) **Cumplimiento,** este es el último dominio y se plantea como una evaluación.

1.2.1 Estado del arte

Gestión de seguridad de la información basado en la norma ISO 27002 en instituciones públicas y privadas

Ayres Sfreddo & Flores (2012) en su artículo "Seguridad de la información de archivos: El control de acceso de archivos Públicos Estatales", explica que la Asociación Brasileña de Técnicas (ABNT) adopto la **NBR ISO/IEC 17799:2005**[2], su objetivo no es crear un modelo de seguridad de la información, sino sólo guiar las acciones de los empleados para garantizar la seguridad institucional y documental, ofreciendo directrices que ayudan en el desarrollo de una política de seguridad de la información, con lo cual se evita modificaciones,

[1] "SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización." (El portal de ISO 27002 en Español, 2012 - 2016)
[2] También conocida como ISO 27002

manipulaciones o fraude y garantizando la disponibilidad para los usuarios autorizados, cuando se solicite.

Es importante señalar que la política de seguridad de la información sufre cambios entre instituciones, en base a los objetivos y metas. Así, con el fin de obtener un resultado muy eficaz con esta política, es necesario aplicar algunas cuestiones técnicas que a menudo son comunes entre instituciones, las más aplicadas son, consulta de la información como un bien institucional, poseer un control del acceso a la información, mantener las responsabilidades a los usuarios, la administración y gestión de la información[3], estar preparados para situaciones de contingencia y garantizar la privacidad del usuario, por último, definir medidas disciplinarias si se infringen las reglas. (Medeiros, 2001)

En la investigación Ayres Sfreddo & Flores (2012) en los: Archivos Públicos del Distrito Federal, Paraná, Estado de Espírito Santo, Estado de Rio Grande Do Sul, y del Estado de São Paulo se evidencia que existe una política de control de la seguridad de la información, y que sólo una de estas instituciones presento, falencias en la política de control de acceso, aun así, esta institución está llevando a cabo acciones para remediar este problema, a nivel general dentro de estas instituciones se considera que la política de control de acceso es uno de los puntos más críticos el cual debe ser planificado y ejecutado en las instituciones para contribuir a la protección de la información.

Silva Netto & Pinheiro da Silveira (2016) en su artículo "Gestión de la seguridad de la información: factores que influencian su adopción en pequeñas y medianas empresas" expresan que no existe mucha documentación sobre la adopción de la gestión de la seguridad de la información en organizaciones medianas o pequeñas, sin embargo, debido a que la mayoría de las empresas entienden la seguridad de la información como simplemente seguridad de red o seguridad en TI, se utilizó un método exploratorio-descriptivo para la realización de un estudio, fue seleccionado el sector de fabricación de productos de metal, localizado en la región del ABC paulista, con 256 empresas registradas, siendo 225 clasificadas como empresas de pequeño porte y 31 empresas clasificadas como medio porte.

> Se obtuvo los siguientes datos en la capa física utilizan herramientas como el antivirus, presente en el 100% de las empresas encuestadas, seguido por el sistema de copia de seguridad (97,6%) y firewall (82,9%), la capa humana carece

[3] Hace referencia a que el director un área es responsable por el uso de sistemas y servicios de información que presta

> de atención por parte de las empresas, pues fue la que presentó el menor índice de controles implantados, los datos confirman que las empresas invierten principalmente en controles tecnológicos para disminuir el riesgo de incidentes de seguridad de la información, pero olvidan que el factor humano es uno de los grandes responsables de fallas en la seguridad, en cuanto a las secciones de la norma ISO IEC 27002: 2005, se verificó una baja adecuación de las pequeñas y medianas empresas, lo que puede demostrar que la norma requiere muchos controles que la mayoría no está preocupada por implantar o no tiene tiempo o dinero para ello, en cuanto a la norma sugiere 127 controles y en este trabajo se seleccionaron solamente 20. (Silva Netto & Pinheiro da Silveira, 2016, p. 21)

Silva Netto & Pinheiro da Silveira (2016) concluyen que las pequeñas y medianas empresas, a pesar de considerar la pérdida financiera como el principal factor para la adopción de la gestión de la seguridad de la información, carecen de conocimientos sobre la correcta gestión de la seguridad de la información.

Gestión de la seguridad de la información Familia ISO 27000 a nivel mundial

Disterer (2013) en el artículo "ISO/IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información" explica que estas normas constituyen un marco para el diseño y el funcionamiento de un SGSI, basándose en experiencias de desarrollo duradero, con esto las empresas tienen oportunidad de alinear sus procedimientos y métodos para garantizar un nivel adecuado de seguridad de la información con un estándar internacional.

La figura, expone el número de certificaciones ISO 27001 por región:

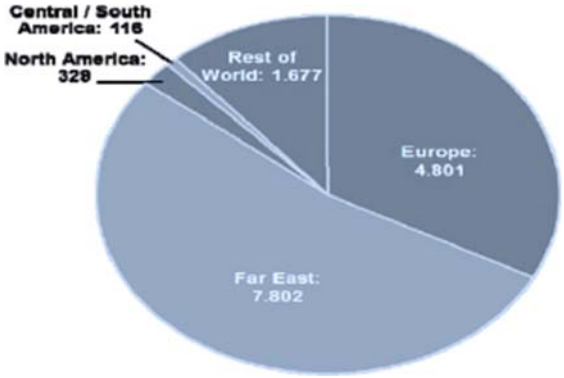


Figura 3. Certificados ISO 27001 por región

Fuente: (Disterer, 2013)

El alto número de certificaciones en Asia se da porque las empresas en Europa y América del Norte están reduciendo los costos a través de la externalización de servicios de TI.

"La certificación en ISO 27001 en Sudamérica ha llevado una progresión creciente, en el año 2006 sólo existían 18 certificados, en 2010 ya eran 117 certificado y **en el año 2016 la cifra ascendió a 564 certificado,** esto supuso **un incremento del 1,7%** en 10 años." (SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información, 2017)

Franco & Guerrero (2016) en su artículo Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002, detallan que el uso de la norma a nivel de empresas colombianas se encuentra de la siguiente manera:

Herramienta	BABEL	E-PULPO	MEYCOR COBIT KP	SECUWARE SECURITY	GLOBALSGSI	GXSGSI	GAP ISO 27001	SECURIA SGSI
Creador	ÁRTICA	INGENIA	DATASEC	SECUWARE	AUDISEC	SIGEA	SIGEA	SECURIA
Licencia	Open Source	GNU GPL v2	Comercial	Comercial	Comercial	Comercial	Comercial	GPL v2
Sistemas operativos en los que funciona	GNU/Linux, IBM AIX, Sun Solaris, OpenSolaris, SPARC, Windows	GNU/Linux	Windows	Windows	Windows	Windows	Windows	GNU/Linux, Windows
Estándares de seguridad	SOX/LOPD, ISO 27001, COBIT	ITIL, LOPD, ENS, ISO 27001, ISO 27002, ISO 20000	ISO 127001, COBIT, ISO 27002, ISO 20000, COSO I, COSO II	Ninguno. Suite empresarial para proteger la información en el puesto de trabajo.	ISO 27001	UNE 71502, ISO 27001	ISO 27001, ISO 27002	ISO 27001
Gestión documental	✓	✓	✓	×	✓	×	×	✓
Gestión de incidencias	✓	✓	✓	×	✓	✓	×	✓
Auto-evaluación de controles	✓	×	✓	×	✓	×	×	✓

Figura 4. Contrastación de los sistemas de apoyo a SGSI existentes en Colombia
Fuente: (Franco & Guerrero, 2016)

Tomando como precedente la figura 4, la mayoría de herramientas de software existentes para el apoyo de los Sistemas de Información (SI) de una organización son propias de firmas de auditoría, son restringidas y costosas, al ser desarrolladas por este tipo de firmas, la licencia es de tipo comercial, lo cual restringe en cierta manera su uso debido a los altos costos de licenciamiento, también se ha detectado que todas están basadas en el estándar ISO 27001 y algunas tienen incorporados otros estándares como COBIT, ITIL, LOPD, pero son muy pocas las que están directamente relacionadas con ISO 27002. (Franco & Guerrero, 2016)

Mejores prácticas de TI

Arora (2010) explica que elegir el correcto marco de normas para la gobernabilidad, la seguridad de la información y el cumplimiento de las mejores prácticas de la industria se ha convertido en el nuevo dilema de los gerentes. La figura 6 muestra una comparación entre Cobit, ITIL e ISO 27000:

ÁREA	CobiT	ITIL	ISO 27000
Funciones	Mapeo de procesos IT	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de referencia de seguridad de la Información
Áreas	4 Procesos y 34 Dominios	9 Procesos	10 Dominios
Creador	ISACA	OGC	ISO International Organization for Standardization
¿Para qué se implementa?	Auditoría de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad
¿Quiénes lo evalúan?	Compañías de contabilidad Compañías de consultoría en IT	Compañías de Consultoría en IT	Compañías de Consultoría en IT, Empresas de Seguridad Consultores de seguridad en redes

Figura 5. Comparación entre Cobit, ITIL e ISO 27000
Fuente: (Montaño Orrego, 2011)

Ionescu (2016) explica que las organizaciones que deseen adoptar las mejores prácticas de TI necesitan una gestión eficaz, un marco que proporciona un enfoque global coherente y que garantice resultados comerciales exitosos cuando se usa TI para respaldar la estrategia de la empresa, **COBIT** se enfoca en lo que una empresa necesita hacer, no cómo debe hacerlo, su audiencia es la administración comercial sénior, la alta gerencia de TI y los auditores, a menudo se conoce como el "integrador", llevando vincular estas prácticas de TI con los requisitos del negocio, **ITIL** se basa en la gestión de servicios de TI, se enfoca en el método y define un conjunto más completo de procesos. proporciona un contexto estratégico para la toma de decisiones de TI, **ISO / IEC 27002** es la guía para mantener estándares de seguridad y mejores prácticas de gestión dentro de una organización, la norma enfatiza la importancia de la gestión de riesgos y hace claro que no es necesario implementar todas las pautas establecidas, solo aquellas que son pertinentes.

Los involucrados en el proceso de TI se preguntan: ¿qué norma debería implementarse primero? Desafortunadamente, nadie puede dar una solución exacta a este problema, porque depende de los procesos y procedimientos de TI de la compañía y en sus requisitos, es cierto que la mayoría de las empresas comienzan a implementar COBIT primero porque estos estándares cubren en general todos los sistemas de información, y después de eso, si es necesario, eligen entre ITIL e ISO27002, el presupuesto de la empresa también debe tenerse en cuenta porque la implementación de COBIT se ejecuta a partir de una auditoría interna, mientras que ITIL e ISO27002 generalmente se realizan usando el presupuesto del departamento de TI, ahora si analizamos la complejidad ITIL es el estándar más fácil, porque puede funcionar parcialmente sin ningún impacto en el desempeño de la compañía, por otra parte COBIT e ISO27002 son bastante difíciles de implementar parcialmente pues primero deben tener una visión general de todos los procesos y solo entonces pueden funcionar sin problemas. (Ionescu, 2016)

Implementación de la ISO 27001

Valencia-Duque & Orozco-Alzate (2017) en su artículo "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000" explica que para lograr cierto nivel de éxito, disminuir la incertidumbre en sus resultados, se necesita, tiempo, recursos, apoyo de la alta dirección y cumplir con 5 faces secuenciales, que se detallan a continuación:

Fases 27003:2010	Etapas	Numerales de la norma ISO/ IEC 27001:2013 relacionados
Obtener la aprobación de la Dirección para iniciar el proyecto	Establecimiento de las prioridades de la organización para desarrollar un SGSI	4.1. Conocimiento de la organización y de su contexto.
	Definir el alcance preliminar del SGSI	4.2. Comprensión de las necesidades y expectativas de las partes interesadas.
	Creación del plan del proyecto para ser aprobado por la Dirección	5.1. Liderazgo y compromiso 7.1. Recursos
Definir el alcance, los límites y la política del SGSI	Definir el alcance y los límites del SGSI	4.3. Determinación del alcance del sistema de gestión de seguridad de la información.
	Definir el alcance y los límites de las Tecnologías de Información y Comunicaciones	
	Definir el alcance y los límites físicos	
	Integrar cada alcance y los límites para obtener el alcance y los límites del SGSI	
	Desarrollar la política del SGSI y obtener la aprobación de la Dirección	5.1. Liderazgo y compromiso 5.2. Política 6.2. Objetivos de seguridad de la información y planes para lograrlos.
	Definición de roles, responsabilidades del SGSI	5.3. Roles, responsabilidades y autoridades en la organización. 7.2. Competencia 7.3. Toma de conciencia
Realizar el análisis de los requisitos de seguridad de la información	Definir los requisitos de seguridad de la información para el proceso SGSI	4.2. b) La organización debe determinar los requisitos de las partes interesadas pertinentes a la seguridad de la información.
	Identificar los activos dentro del alcance del SGSI	
	Realizar una evaluación de la seguridad de la información	6.1.2. Valoración de riesgos de seguridad de la información.
Realizar la valoración de riesgos y planificar el tratamiento de riesgos	Realizar la valoración de riesgos	6.1.2. Valoración de riesgos de seguridad de la información.
	Seleccionar los objetivos de control y los controles	6.1.3. Tratamiento de riesgos de la seguridad de la información. 6.2. Objetivos de seguridad de la información y planes para lograrlo.
	Obtener la autorización de la Dirección para implementar y operar el SGSI	5.1. Liderazgo y compromiso

Diseñar el SGSI	Diseñar la seguridad de la información de la organización	7.4. Comunicación
	Diseñar la seguridad física y de las Tecnologías de Información y Comunicaciones	7.5. Información documentada
	Diseñar la seguridad específica de un SGSI	8.1. Planificación y control operacional
	Producir el plan del proyecto final del SGSI	8.2. Valoración de riesgos de seguridad de la información.
		8.3. Tratamiento de riesgos de seguridad de la información.
		9.1. Seguimiento, medición, análisis y evaluación
		9.2. Auditoría interna
		9.3. Revisión por la Dirección

Figura 6. Fases de implementación de un SGSI y su relación con los numerales de la norma ISO/IEC 27001:2013

Fuente: (Valencia-Duque & Orozco-Alzate, 2017)

1.2.2 Adopción de una Perspectiva Teórica

Esta investigación adoptará la metodología ISO 27002, según los estudios de Ayres Sfreddo & Flores (2012) en empresas públicas y privadas de Brasil concluyen la viabilidad de esta norma y sus resultados son altamente efectivos, lo que permite guiar las acciones de los empleados garantizando; el uso de buenas prácticas y la seguridad de la información.

1.2.3 Marco Conceptual

- **ISO 27002**: "El Estándar Internacional ISO/IEC 27002 va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo." (EcuRed, 2011)
- **Políticas de Seguridad de la Información:** "importancia que ocupa la disposición de una adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior." (Sistemas de Gestión de Seguridad de la Información SGSI, 2016)

- **Norma:** "principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad." (Montoya, 2009)
- **Buena práctica:** "son aquellas acciones que se caracterizan por haber logrado cumplir eficazmente las metas planteadas, y que luego de la evaluación de resultados, se ha concluido que proporcionan beneficios óptimos en la mayoría de casos, de modo que se son prácticas replicables y útiles para implementar." (Montoya, 2009)
- **Control de la Información:** "consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización." (SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información, 2015)

1.2.4 Hipótesis

El diseño de una política de seguridad permitirá una mejor gestión de la información por parte del personal del área de TICS de la empresa Flower Village Ecuador.

CAPÍTULO II

ANÁLISIS Y DISEÑO

2.1 Levantamiento de datos

Flower Village Ecuador, es una empresa que comercializa toda su producción a clientes extranjeros, por lo cual está sometida a la certificación de la Alianza Empresarial para el Comercio Seguro BASC (2017) **"la cual busca establecer medidas que prevengan el tráfico de drogas a través de las exportaciones, con el uso de normas para la seguridad de la información y protecciones para el comercio internacional".**

En el año 2017 Flower Village obtuvo la certificación con observaciones a la seguridad de la información área de TICS servicio de storage, la norma ISO 27002 me permite diseñar una política de seguridad como se observa en la figura 8 y posteriormente buscar una certificación con el uso de la ISO 27001.

Según Avilés Armijos & Uyaguari Guartatanga (2012) La Política de Seguridad tiene dos propósitos centrales, informar a todos los usuarios sobre las obligaciones que deben asumir respecto a la seguridad asociada a los recursos de tecnología de información y dar las guías para actuar ante posibles amenazas y problemas presentados. (pp. 1-2)

La Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, por ende, debe estar avalado y contar con un fuerte apoyo de la dirección y/o máxima gerencia, ya que, sin este apoyo, su diseño o implementación será más compleja e incluso puede fracasar. (Burgos Salazar & Campo, 2009, pp. 241-242)

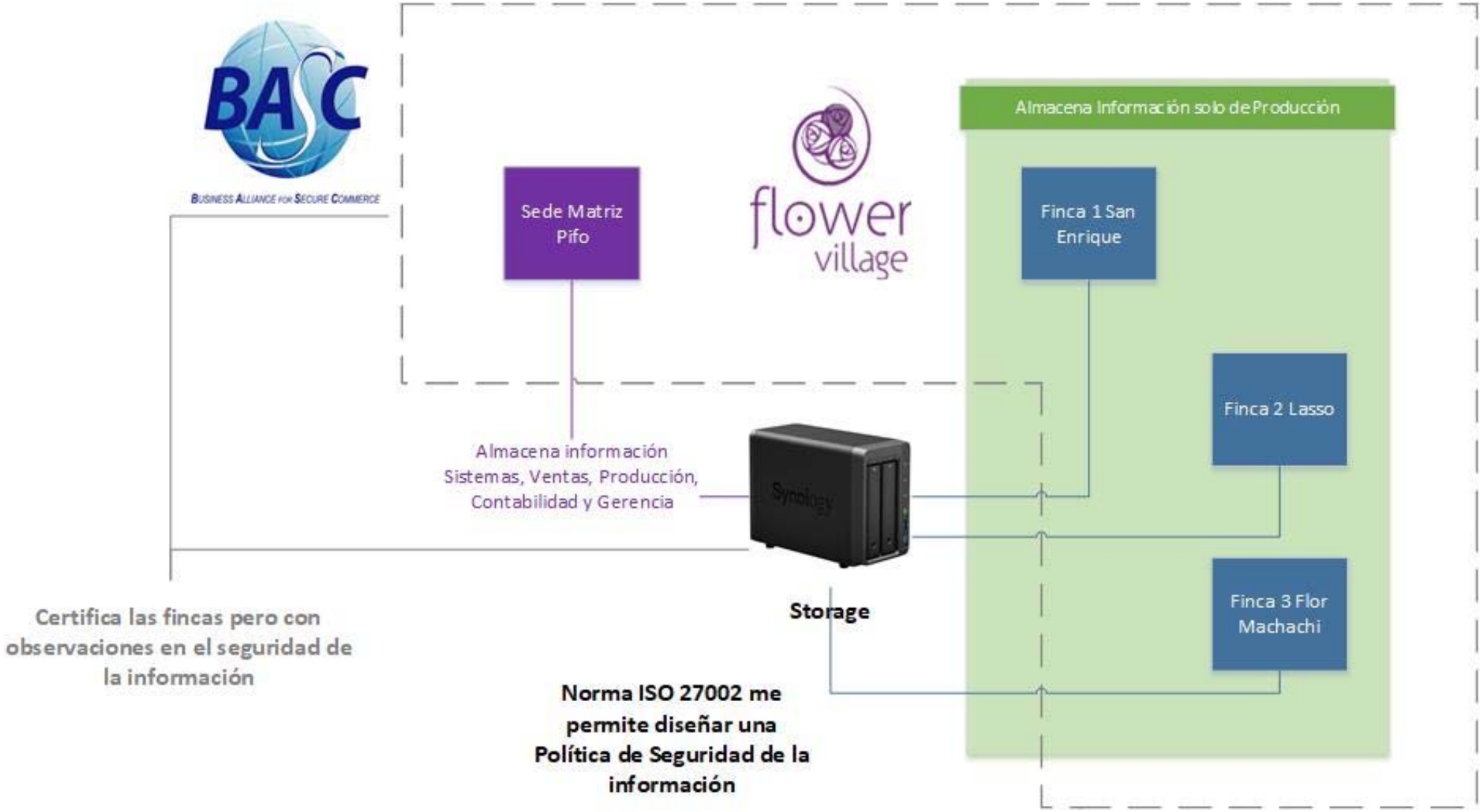


Figura 7. Certificación que provee BASC a Flower Village Ecuador

Elaborado por: Autor de la Investigación

Es necesario explicar que existen factores puntuales, para que una política de seguridad de la información falle:

- La gerencia no termina de comprender la necesidad y los beneficios
- El personal que diseña la política no tiene claro los procesos y procedimientos.
- Cambio de autoridades, las cuales pueden pedir que se replantee el trabajo ya realizado o en marcha

Finalmente, es importante señalar que una política no garantiza completamente la seguridad dentro de una empresa, lo que busca con la misma es la prevención, concientizar y capacitar a los usuarios, con el fin de satisfacer las necesidades de la organización.

"Es muy frecuente que todo aquél que se interesa por primera vez en la serie ISO 27000 se encuentre con algún problema al delimitar y entender las fronteras y los ámbitos de las dos principales normas que la componen." (Benjumea, 2016)

Es fundamental entender que la seguridad de la información es un ámbito que debe incluir el compromiso y capacitación de los usuarios, pues la **confidencialidad, integridad y disponibilidad,** permite mantener y mejorar un SGSI.

Como se explicó en el estado del arte, la serie ISO 27000, es la opción más socorrida por su relación con la Seguridad de la Información, entre las que destacan la ISO 27001 y la ISO 27002.

La siguiente figura ofrece una visión general de las diferencias entre la ISO 27001 y la ISO 27002

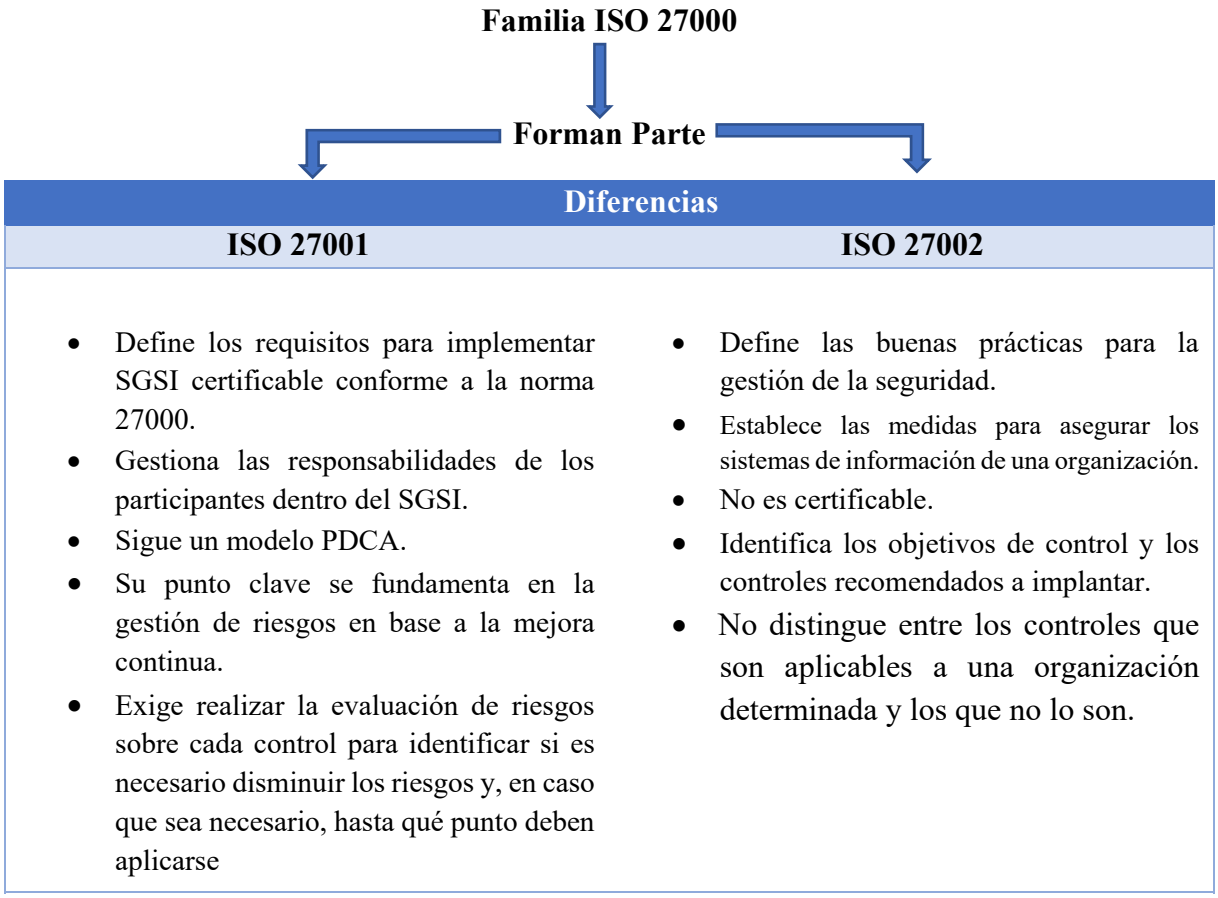


Figura 8. Diferencias ISO 27001 & ISO 27002

Elaborado por: Autor de la Investigación

"La pregunta es: ¿Por qué existen ambas normas en forma separada, porque no han sido integradas utilizando los aspectos positivos de cada una? La respuesta está en la utilidad: si fuera una única norma, sería demasiado compleja y larga como para que sea práctica." (Kosutic, 2017). Se puede entonces establecer que estas dos normas se complementan mientras que la ISO 27001 se enfoca en la administración, la ISO 27002 proporciona controles, así como una descripción de cómo usarlos; su uso por separado o en conjunto debe ser una decisión que parte de cada departamento de TI y expuesto tanto a la alta gerencia como a los distintos departamentos.

2.2 Matriz de Riesgos

El uso de la matriz de riesgos permite identificar riesgos potenciales, en el caso particular de la empresa Flower Village Ecuador, es necesario analizar la administración del storage por parte del área de TICS y su incidencia en los usuarios que la usan este servicio.

Nro. De Ref.	Descripción del problema	Riesgo	Fecha de Identificación	Tipo de Riesgo		Categoría de Riesgo	Objetivo de proyecto afectado				Tipo de Impacto		Probabilidad	Valoración de Impacto				Probabilidad por Impacto				Valoración Global Riesgo	Prioridad	Dueño (Owner)	Plan de Respuesta predeterminado
				Amenaza	Oportunidad		Alcance	Tiempo	Costo	Calidad	Directo	Indirecto		Alcance	Tiempo	Costo	Calidad	Alcance	Tiempo	Costo	Calidad				
1	Los usuarios tienen acceso a toda la información que se almacena	Perdida de información	05/01/2018	X		Equipo de Trabajo		X			X		5	0	1	1	0	0	5	5	0	4	Alta	TICS	Establecer parámetros para acceso a la información por departamento
2	No existe niveles de acceso y segmentación por carpetas según el departamento	Confusión y perdía de tiempo al localizar la información	08/01/2018		X	Equipo de Trabajo		X			X		5	0	1	1	0	0	5	5	0	4	Alta	TICS	Diseñar un árbol para el manejo de la información dentro del storage
3	Las credenciales no son seguras, las mismas se han propagado entre los usuarios	Cada usuario puede usar sus credenciales o las que le hayan proporcionado terceros	10/02/2018		X	Tecnológico		X			X		5	0	1	1	0	0	5	5	0	4	Alta	TICS	Crear nuevas credenciales y niveles de acceso para las mimas según el grado jerárquico en la empresa
4	Existe un único respaldo	Falla en el storage	05/01/2018	X		Tecnológico			X		X		5	0	1	1	0	0	5	5	0	4	Alta	TICS	Adquirir un servicio de terceros para almacenar la información
5	Los archivos, se han borrado, no se han actualizado o no muestran la información que se necesita para trabajar	No existe un control en el manejo de la información	22/02/2018	X		Equipo de Trabajo			X		X		5	0	1	1	0	0	5	5	0	4	Alta	TICS	Establecer permisos de acceso

Figura 9. Matriz de Riesgos

Elaborado por: Autor de la Investigación

Los riesgos, que se enlistan se identificaron en las reuniones con los representantes de cada área, tomando en cuenta su experiencia y los cuellos de botella que experimentaron en temporada de Valentin 2017, Madres 2017 y Valentin 2018 – las actas completas no se pueden incluir en este documento, solo se anexara el punto que hace referencia a la descripción del problema que aparece en la matriz de riesgos

2.3 Grupo de estudio

Como se pudo observar en la figura 7, varios departamentos almacenan, actualizan o eliminan información dentro del storage, mientras que en la figura 10, se puede observar que solo existe una única carpeta **(PUBLICA),** donde todos los usuarios realizan sus respectivas actividades.

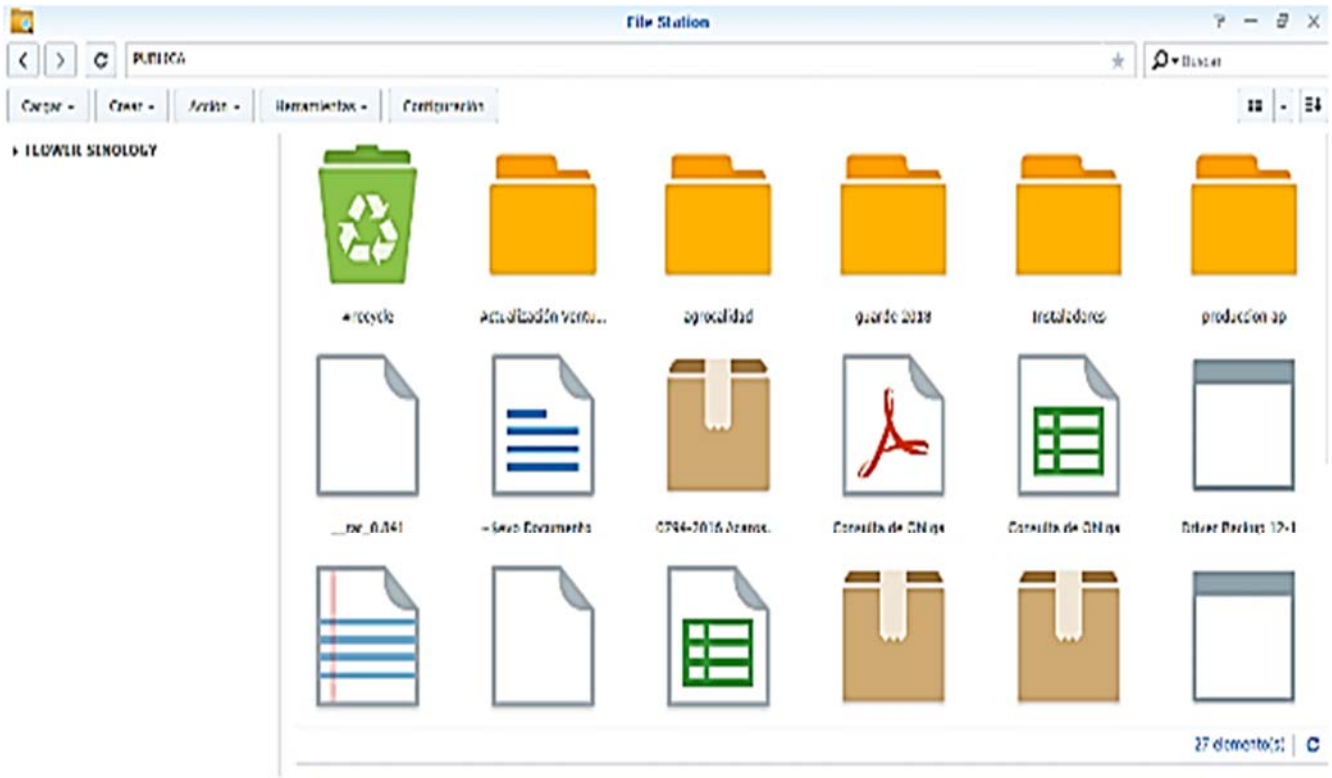


Figura 10. Estructura de archivos storage
Elaborado por: Autor de la Investigación

Cada usuario que ingresa al storage utiliza unos de los 3 perfiles (figura 11) que se encuentran creados.

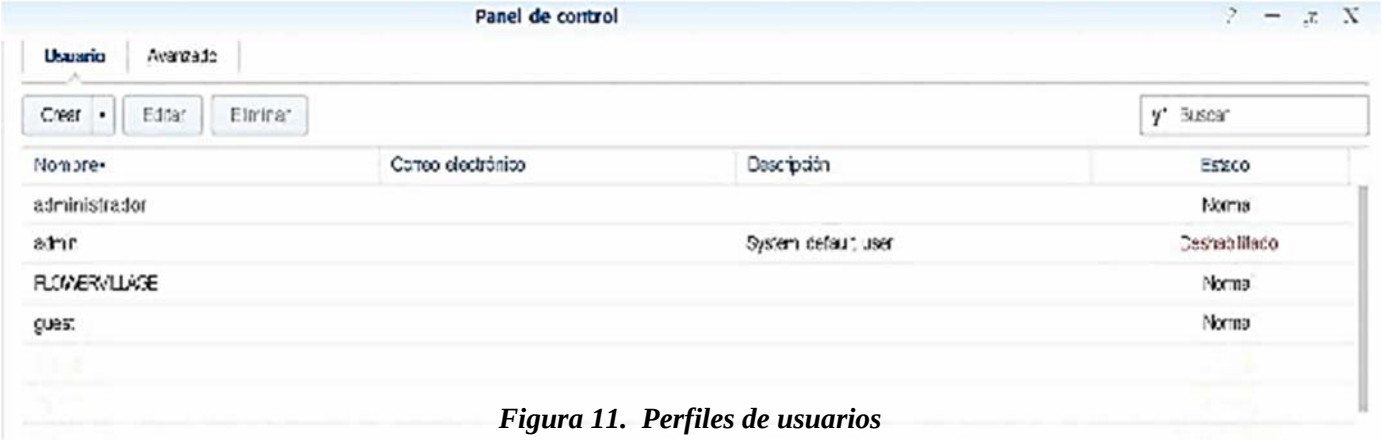


Figura 11. Perfiles de usuarios
Elaborado por: Autor de la Investigación

De un total de 77 equipos, distribuidos entre las fincas; se obtuvieron los siguientes datos:

- 47 equipos, tienen un acceso automático pues las credenciales están guardadas
- 30 equipos, deben colocar las credenciales, no se pudo determinar el número total de personas que disponen de esta información.

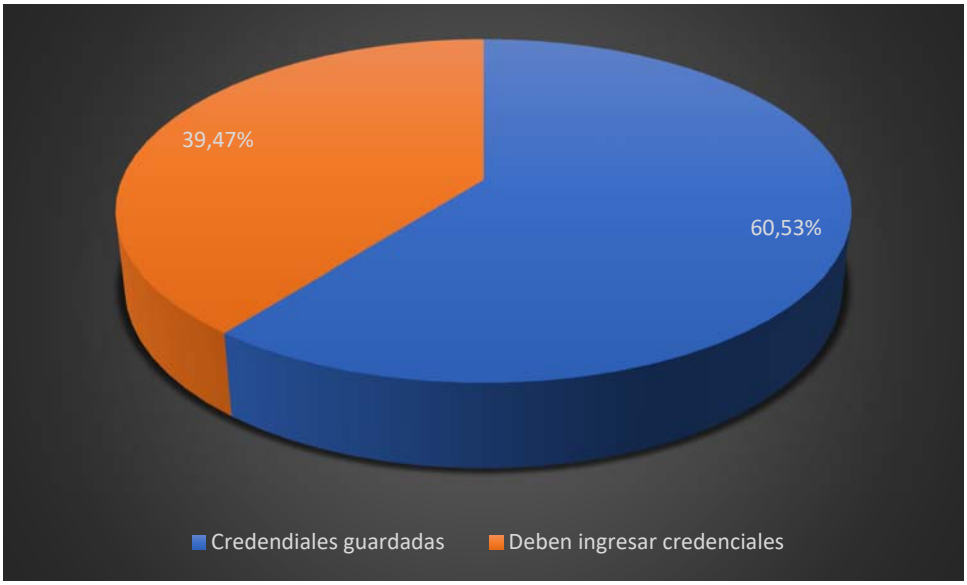


Figura 12. Porcentaje de equipos que pueden acceder al storage
Elaborado por: Autor de la Investigación

Según la información recopilada y con el apoyo de la alta gerencia, se optó por seleccionar a dos personas, analizando el cargo y la antigüedad; las mismas a quienes se les entregaran credenciales y capacitación para ingresar al storage, teniendo en cuenta que su puesto les obliga hacerlo desde las distintas fincas.

El funcionamiento del servicio de storage, parte de la sugerencia que propuso la alta gerencia de seleccionar a 12 usuarios, los mismos serán creados por el área de TICS y asignados al departamento que correspondan (gerencia, contabilidad, ventas, producción y sistemas), posteriormente se asignarán permisos por carpetas, para lectura y escritura de la información como se detalla en el siguiente flujo de datos:

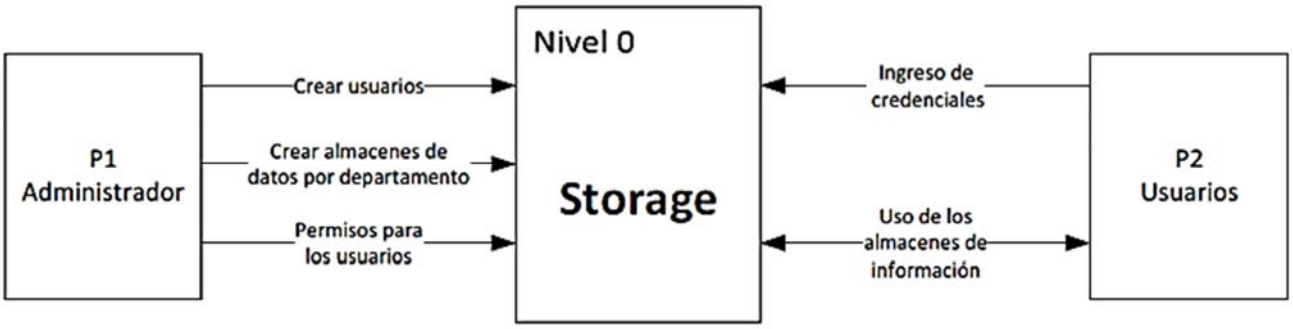


Figura 13. Diagrama de Contexto
Elaborado por: Autor de la Investigación

El diagrama de contexto solo explica de forma genérica el funcionamiento del servicio de storage, la figura 15 va más allá y nos muestra la segmentación por niveles de acceso, como se expresa en la figura 14, para definir L (lectura) y LE (lectura/escritura)

	Gerencia		Sistemas		Ventas		Contabilidad		Producción	
Nivel	L	LE	L	LE	L	LE	L	LE	L	LE
Acceso 1	X	X	X	-	X	X	X	X	X	X
Acceso 2	-	-	X	X	X	X	X	X	X	X
Acceso 3										
Ventas	-	-	-	-	X	X			X	X
Producción	-	-	-	-	-	-	-	-	X	X
Contabilidad	-	-	-	-	X		X	X	-	-

Figura 14. Permisos de Acceso
Elaborado por: Autor de la Investigación

Acceso 1 = Gerencia
Acceso 2 = Sistemas
Acceso 3 = Ventas, Producción, Contabilidad

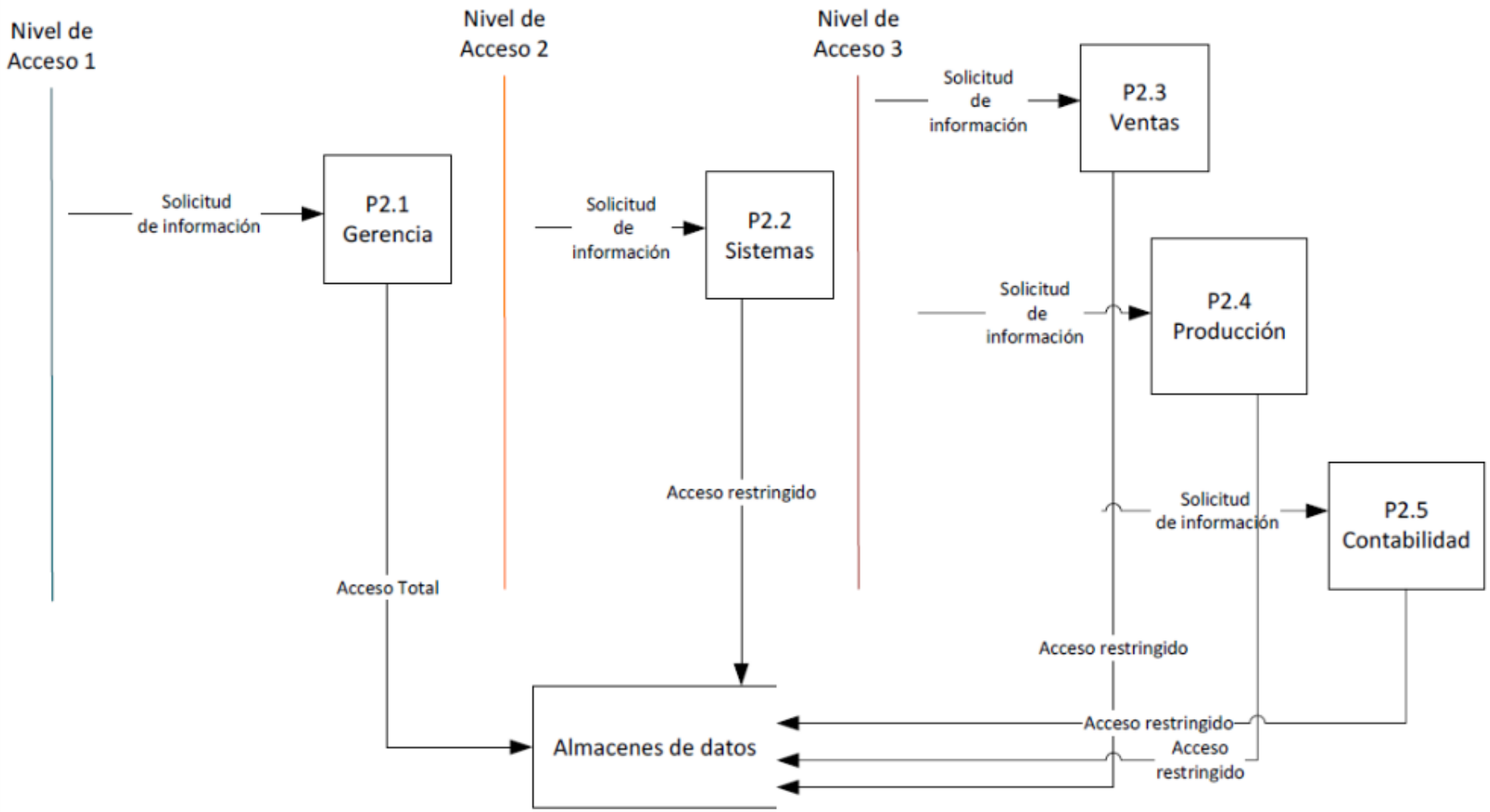


Figura 15. Flujo de datos para permisos de Acceso

Elaborado por: Autor de la Investigación

Este grupo está conformado por 12 personas distribuidas en las siguientes áreas de trabajo como se lo presenta en la figura 16, a quienes se les asignará permisos según el nivel de información que necesiten:

Departamento			
Gerencia	**Cargo**	**Antigüedad**	**Usuario**
Eco. José Miguel Orska	Gerente		jorska
Ing. Nelson Sandoval	G. Financiera		nsandoval
Ing. Guillermo Salcedo	G. Técnica		gsalcedo
Ing. Diego Bonilla	G. Sistemas	4 meses	dbonilla
Contabilidad			
Vicente Arequipa	Contador General	12 años	varequipa
Silvia Allauca	Supervisora Contabilidad	7 años	sallauca
Ventas			
Diego Vega	Jefe Ventas	3 años	dvega
Cristina Davila	Supervisora ventas	2 años	cdavila
Sistemas			
Ing. Henry Almeida	Soporte	8 años	halmeida
Tnlgo. Kevin Cedeño	Soporte	1 año	kcedeno
Producción			
Ing. Jamil Fernández	Jefe Postcosecha	2 años	jfernandez
Roció Chicaiza	Supervisora	5 años	rchicaiza

Figura 16. Personal seleccionado

Elaborado por: Autor de la Investigación

2.4 Análisis del área de TICS

El uso de tecnología dentro de una organización debe ser un proceso planificado orientado a cumplir con las necesidades y objetivos del negocio, así como soportar los procesos clave identificados para la organización.

Flowervillage Ecuador, divide su departamento de sistemas en:

- Gerencia de Sistemas: responsable de gestionar, organizar, planificar y optimizar; los recursos, con fin de cumplir con los objetivos de la empresa.
- Desarrollo, el mismo que se encuentra a cargo de la empresa UNOSOF, hay que puntualizar que este software se orienta al área de producción y ventas, las actualizaciones o requerimientos se gestionan a través del área de TICS

Figura 17. Unosof
Fuente: (UNOSOF, 2008)

- Venture, software ERP adquirido por la empresa y que es de uso exclusivo de contabilidad, bodega y gerencia, los requerimientos se gestionan a través del área de TICS

Figura 18. Venture

Fuente: (Venture, 2005)

- Área de TICS, a cargo de soporte, infraestructura, servidores, storage.

2.4.1 Descripción de las funciones del área de TICS

Como se explicó anteriormente, Flowervillage Ecuador es una empresa que tiene alrededor de 20 años en el mercado, a fines del 2012 la empresa contaba con unos 240 empleados, actualmente se maneja cerca de 600 empleados distribuidos entre las distintas fincas:

- Flowervillage sede Matriz

- San Enrique
- Agroplantas
- Finca Lasso
- Finca Flor Machachi (nueva adquisición diciembre 2017)

Actualmente en el área administrativa se cuenta con 65 empleados y el área de TICS enfoca sus recursos y conocimiento, al cumplimiento de los requerimientos de cada una de las áreas, las personas a cargo son:

- Ingeniero Marcelo Cárdenas (servidores y storage)
- Ingeniero Henry Almeida (soporte e infraestructura)
- Tecnólogo Kevin Cedeño (soporte)

Servidores: actualmente se dispone de cuatro equipos:

Figura 19. Servidor Aplicación Web Unosof
Fuente: Autor de la Investigación

Figura 20. Servidor de Base de Datos Unosof

Fuente: Autor de la Investigación

Figura 21. Servidor ERP Venture

Fuente: Autor de la Investigación

Figura 22. Servidor Firewall
Fuente: Autor de la Investigación

Storage:

Figura 23. Servidor Storage
Fuente: Autor de la Investigación

El área de TICS se encarga del mantenimiento, administración y backup de los distintos, equipos.

Infraestructura

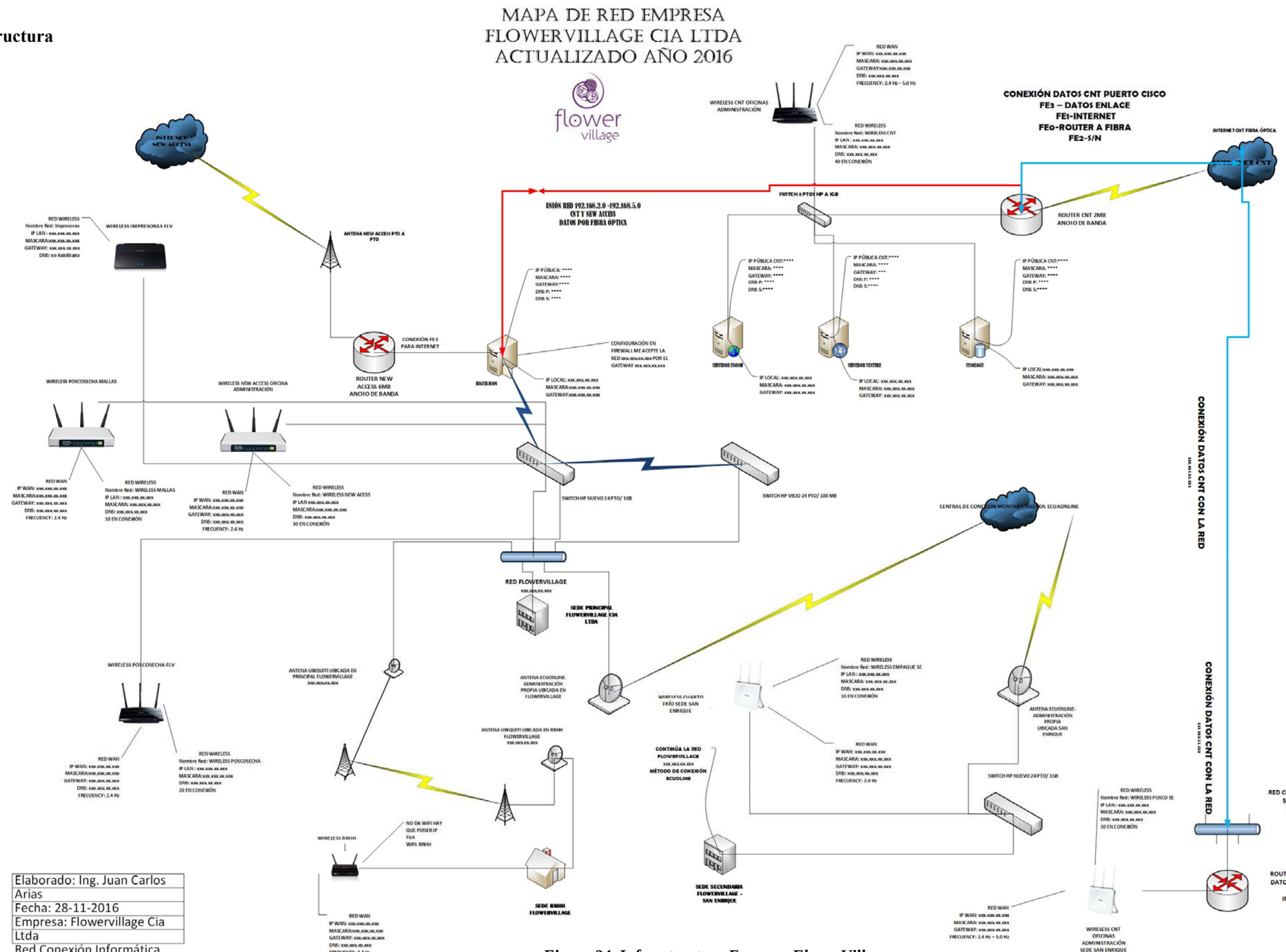


Figura 24. Infraestructura Empresa FlowerVillage
Fuente: Area TICS Flower Village Ecuador

Figura 25. Acceso área de servidores y RAC
Fuente: Autor de la Investigación

La infraestructura cuenta con distintos enlaces como se puede ver en la figura 24, el acceso al área de servidores, rack y sus distintos equipos de comunicación que gestiona la conectividad de la red presentan problemas de seguridad como se muestra en la figura 25.

Todo lo que se ha detallado, se lo ha expuesto a la alta gerencia; en varias reuniones las cuales se siguen manteniendo desde la temporada de Valentín 2018, en la cual a pesar de que la empresa obtuvo buenos dividendos, logísticamente fue un desastre, los cambios que se están proponiendo conllevan tiempo y aún se está analizando cual será el siguiente paso luego de tener una mejor gestión de la información en el servicio de storage.

Soporte: divide sus funciones en:

- Software: Unosof, el personal a cargo posea amplio conocimiento lo que les permite según la figura 24, administrar clientes, crear usuarios, realizar rol back, manejo de inventario, control de producción, generación de reportes, etc., dentro del sistema, no se dispone de acceso al código fuente o a la estructura de la base de datos, por ello a pesar de que el 70% de los requerimientos se solucionan dentro del área de TICS, un 30% solo puede ser solucionado por el personal de Unosof.

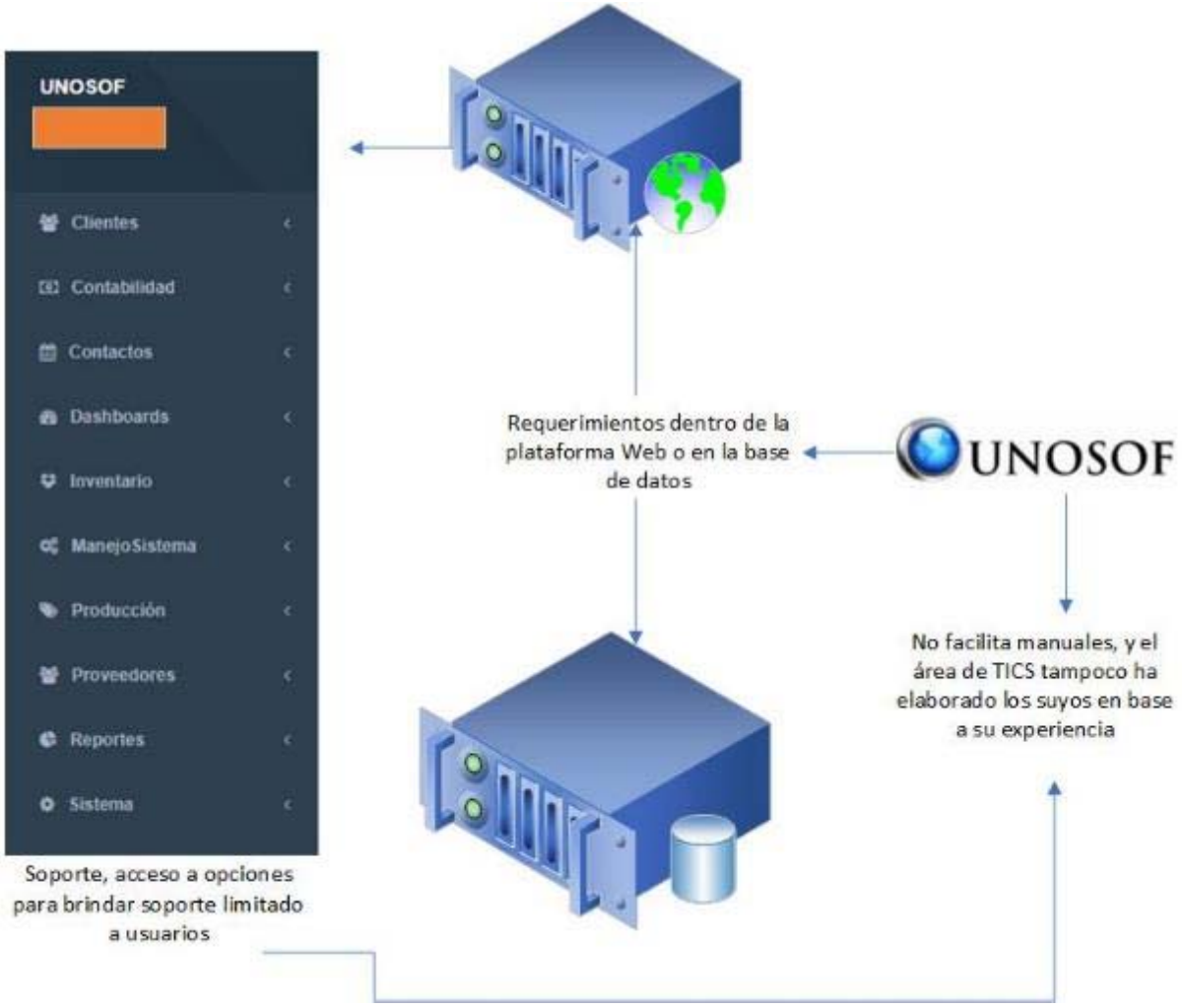


Figura 26. Elementos del Sistema Unosof con los cuales se brinda soporte
Fuente: Autor de la Investigación

La segunda parte lo conforma Venture ERP, el cual posee varios módulos activos antes de la implementación de Unosof, actualmente solo se maneja el módulo de recursos humanos y contabilidad, el soporte para este sistema se aplica en un 80% por parte de la empresa a la cual se adquirió el producto y solo un 20% por parte del área de soporte.

En ambos casos el soporte se da en base al conocimiento del trabajo del día a día, ninguna de las empresas a facilitado manuales y tampoco el área de TICS se ha propuesto en generar documentación, sin embargo por el cambio en la gerencia de sistemas se está generando manuales con base en los incidentes que han sucedido, lo cual servirá de guía para los usuarios y personal del área de TICS.

- Usuarios: orientado a la solución de incidencias en los distintos sistemas operativos, se lo realiza a través de herramientas como el TeamViewer y VNC, hay que recalcar que todos los equipos y herramientas para soporte poseen sus respectivas licencias, no se dispone de un sistema para el manejo de incidencias.

2.5 Objetivos de control de la política de seguridad de la información

2.5.1 Documento de la política de la seguridad de la información

Avilés Armijos & Uyaguari Guartatanga (2012) explican que el contenido de las políticas se basa en el contexto en el que opera una organización, dentro del documento se debe especificar lo siguiente:

- Objetivos de la organización, el alcance y una descripción de la seguridad de la información.
- Valoración y manejo de los riesgos existentes, así como detallar los objetivos de los controles.
- Una descripción de las políticas y normas de conformidad más importantes para la organización. (p. 19)

El portal de la ISO 27002 (2012) explica que el **"documento político"** debe contener:

- **Resumen,** Visión general de una extensión breve, una o dos frases y que pueden aparecer fusionadas con la introducción.
- **Introducción,** breve explicación del asunto principal de la política.
- **Ámbito de aplicación,** descripción de los departamentos, áreas o actividades de una organización a las que afecta/aplica la política.

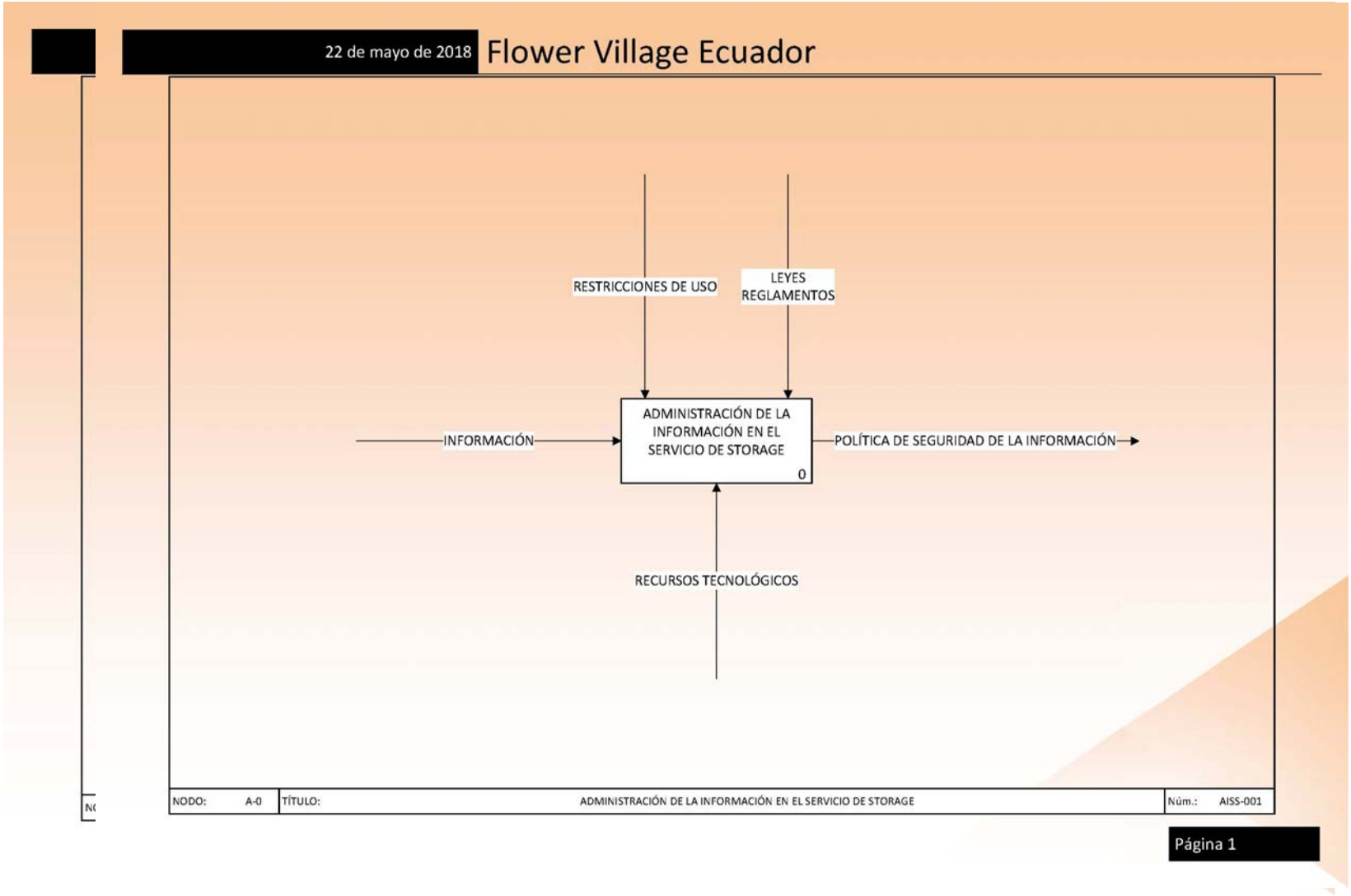
- **Objetivos,** descripción de la intención de la política.
- **Principios,** descripción de las reglas que conciernen a acciones o decisiones para alcanzar los objetivos.
- **Responsabilidades,** descripción de quién es responsable de qué acciones para cumplir con los requisitos de la política.
- **Resultados clave,** descripción de los resultados relevantes para las actividades de la organización que se obtienen cuando se cumplen los objetivos.
- **Políticas relacionadas,** descripción de otras políticas relevantes para el cumplimiento de los objetivos, usualmente se indican detalles adicionales en relación a temas específicos.

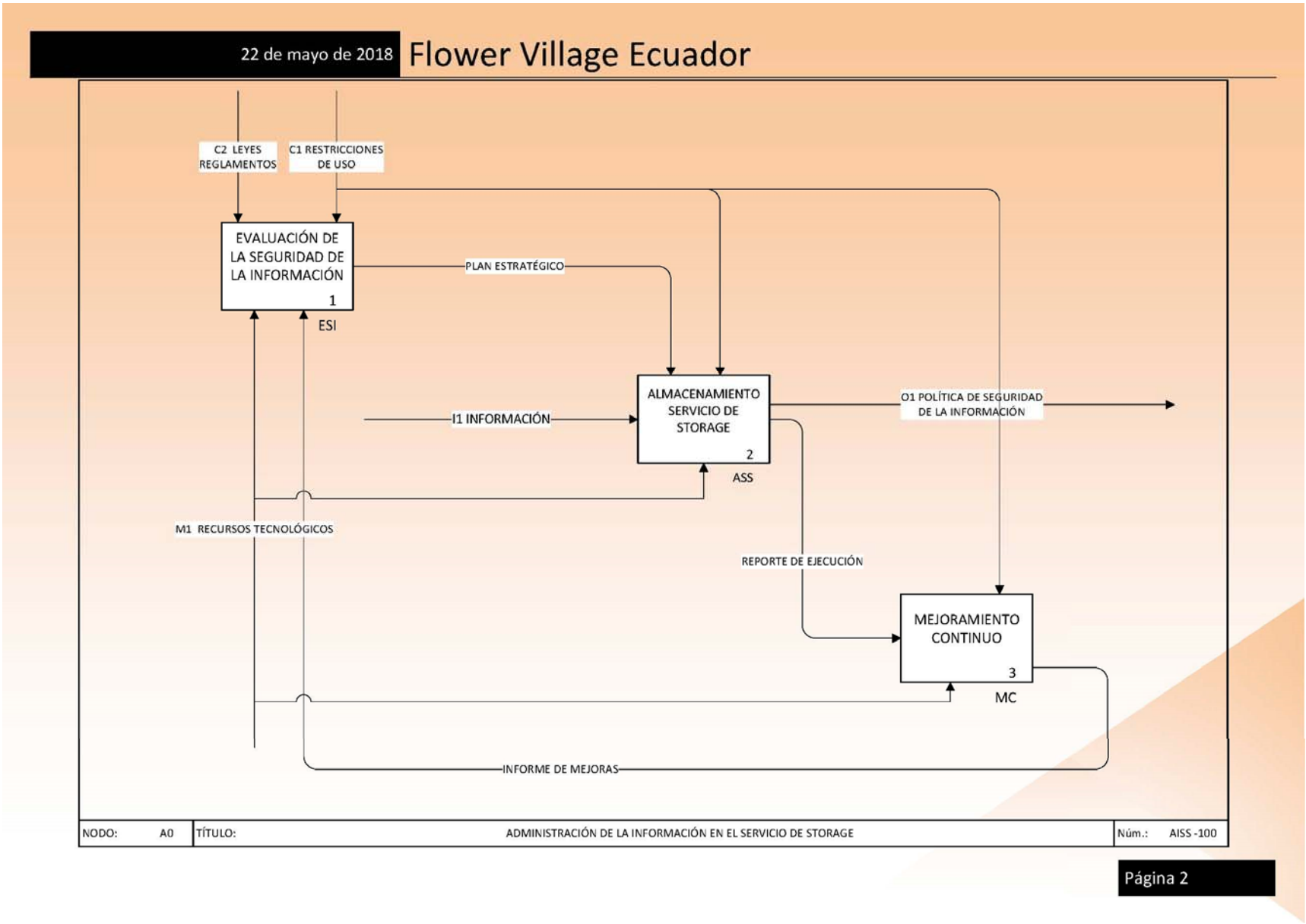
2.5.2 Revisión de la política de seguridad de la información

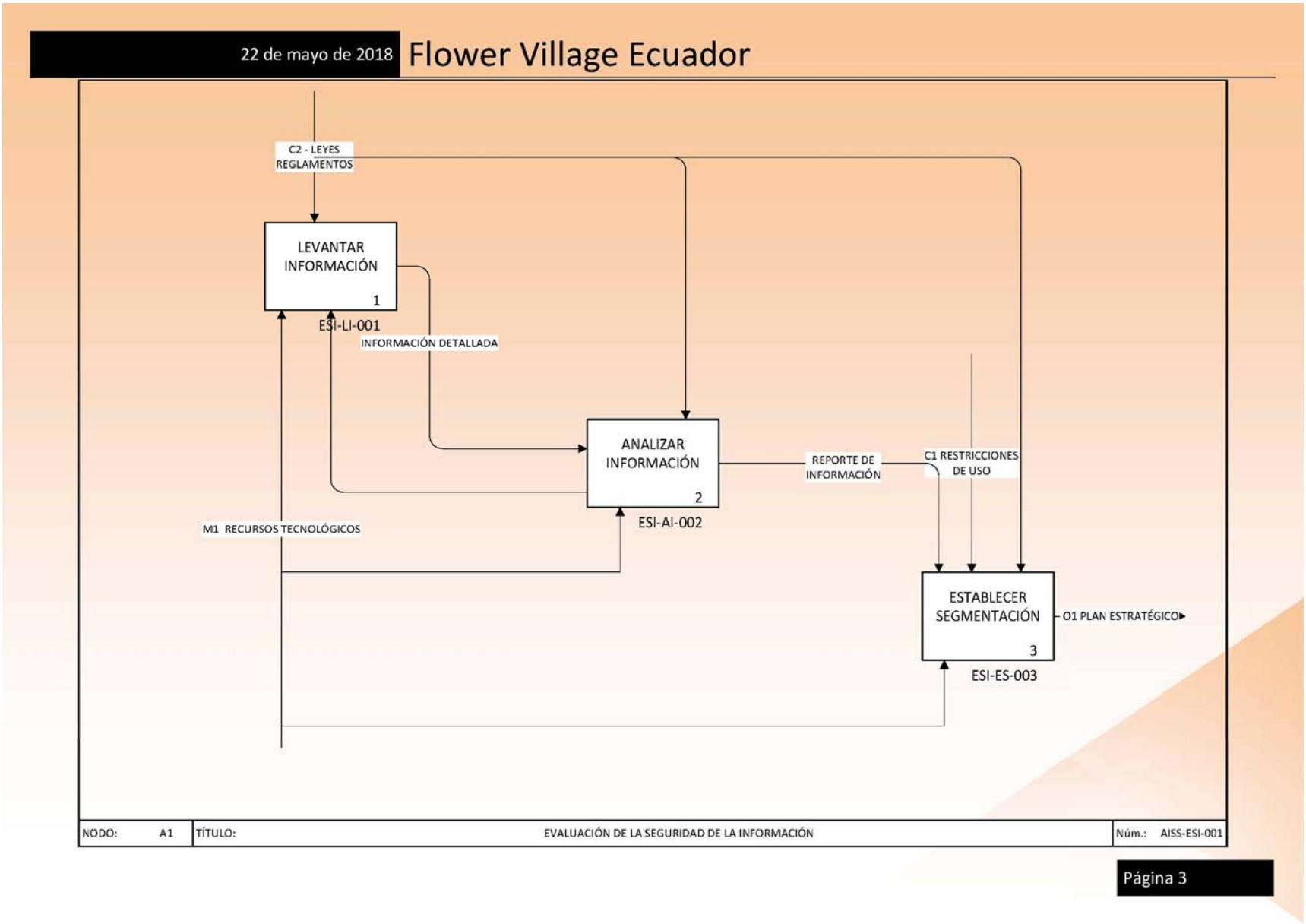
En la revisión de la política de seguridad de la información es necesario indicar los cambios más significativos que repercuten a la primera evaluación de los riesgos presentes en activos de la organización, así como cambios de gran importancia en otros aspectos, esta revisión se debe realizar con cierta frecuencia o en tiempos planificados. (Avilés Armijos & Uyaguari Guartatanga, 2012, p. 19)

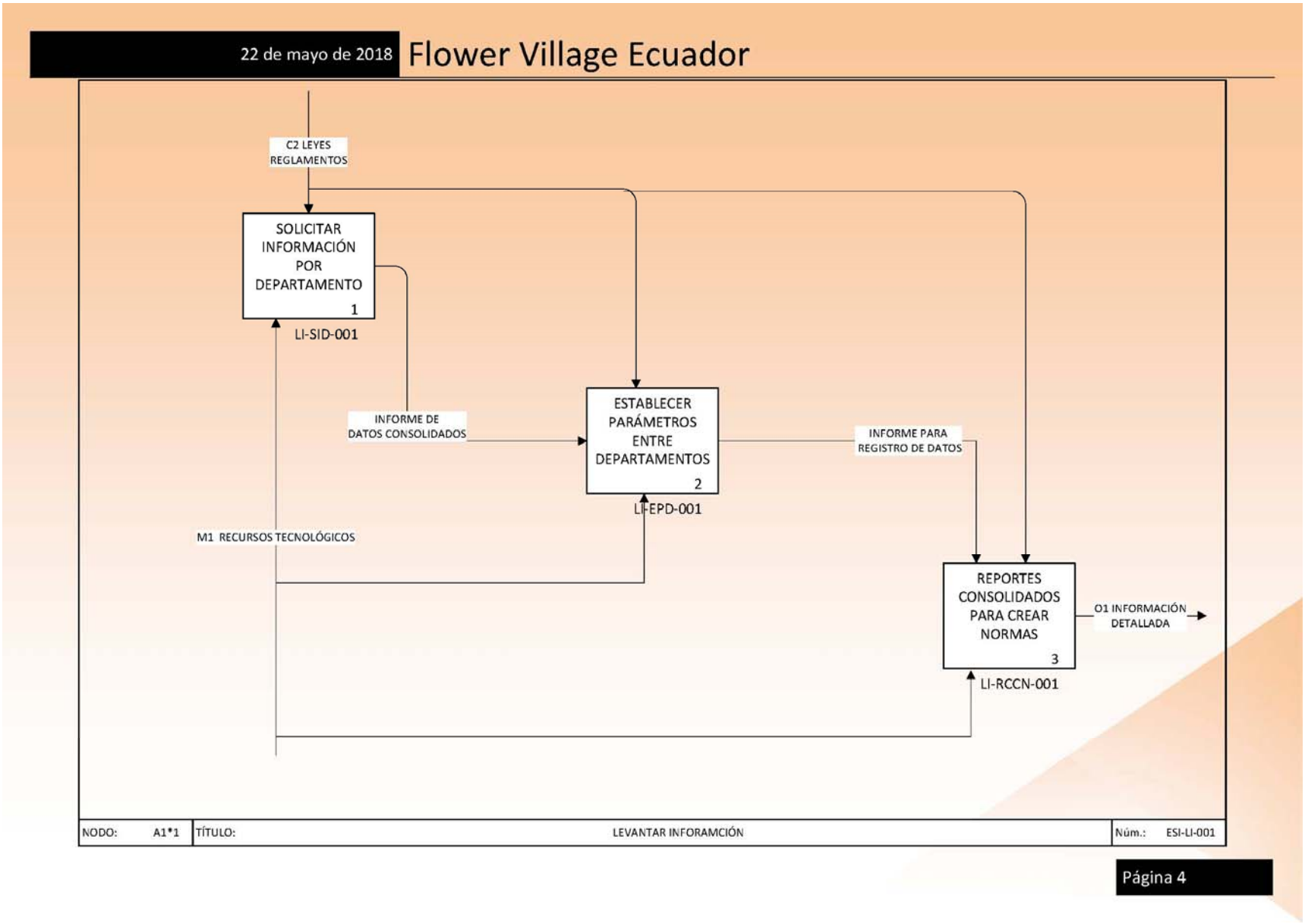
2.6 Presentación de resultados

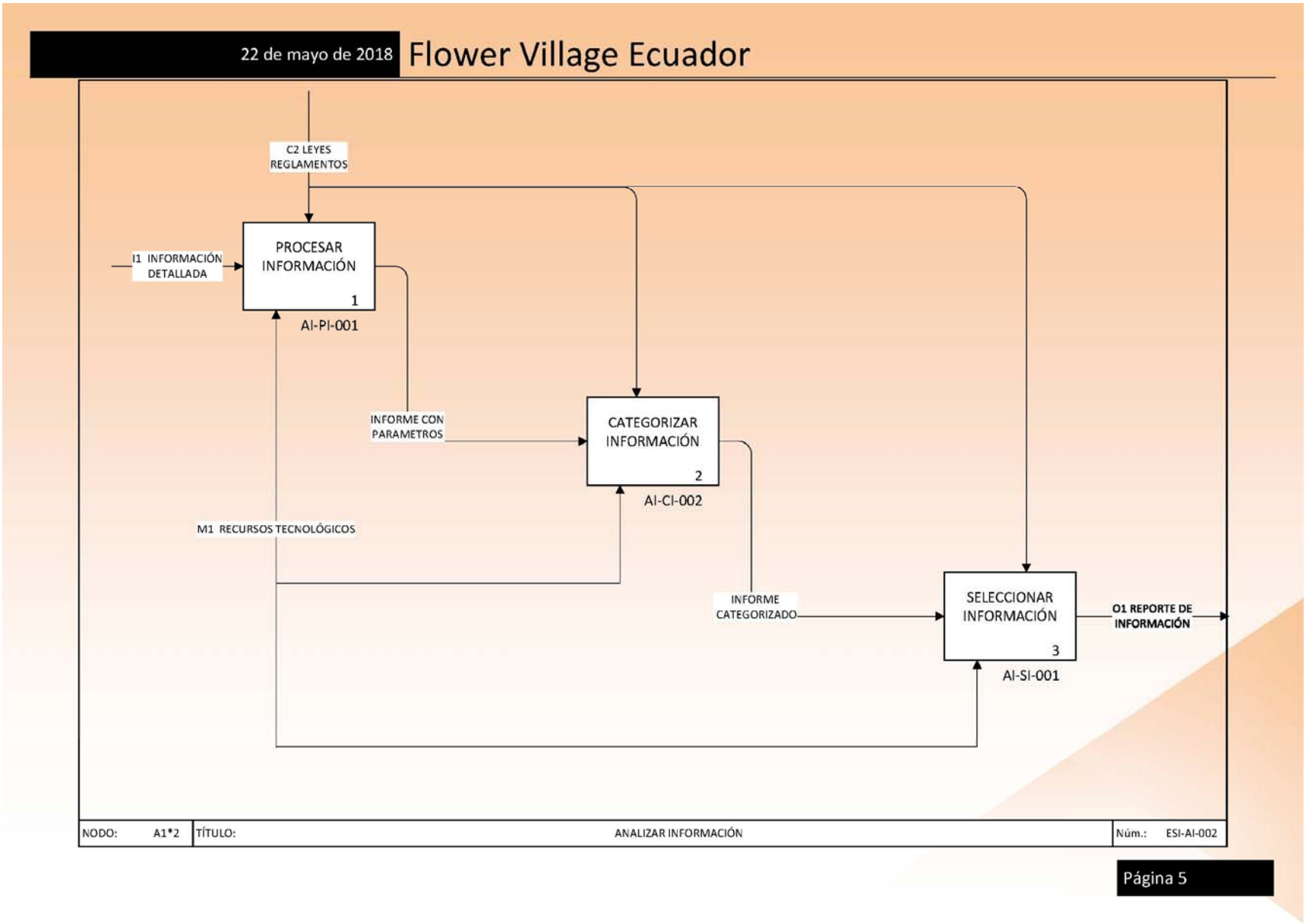
2.6.1 Diagrama de Procesos

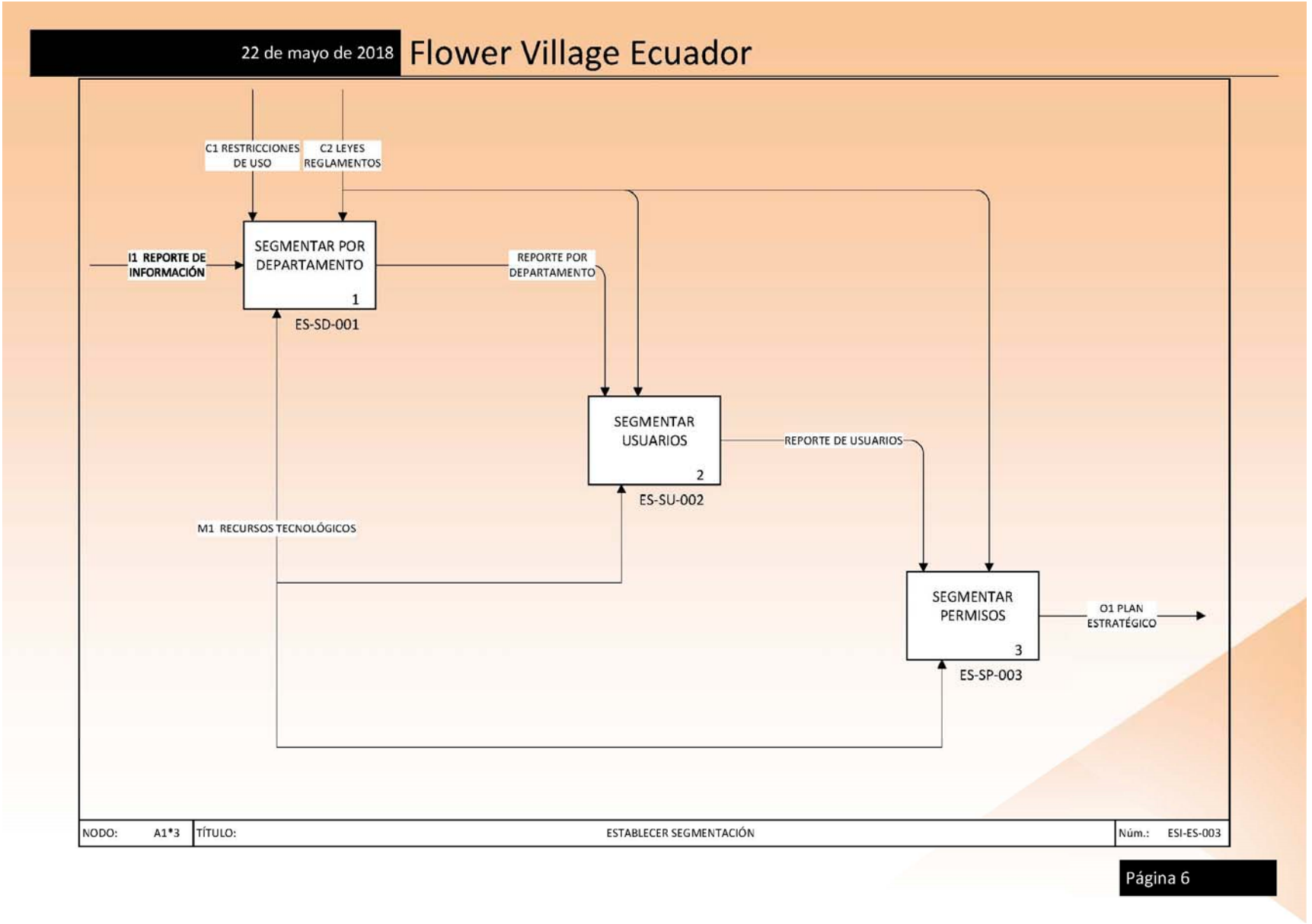


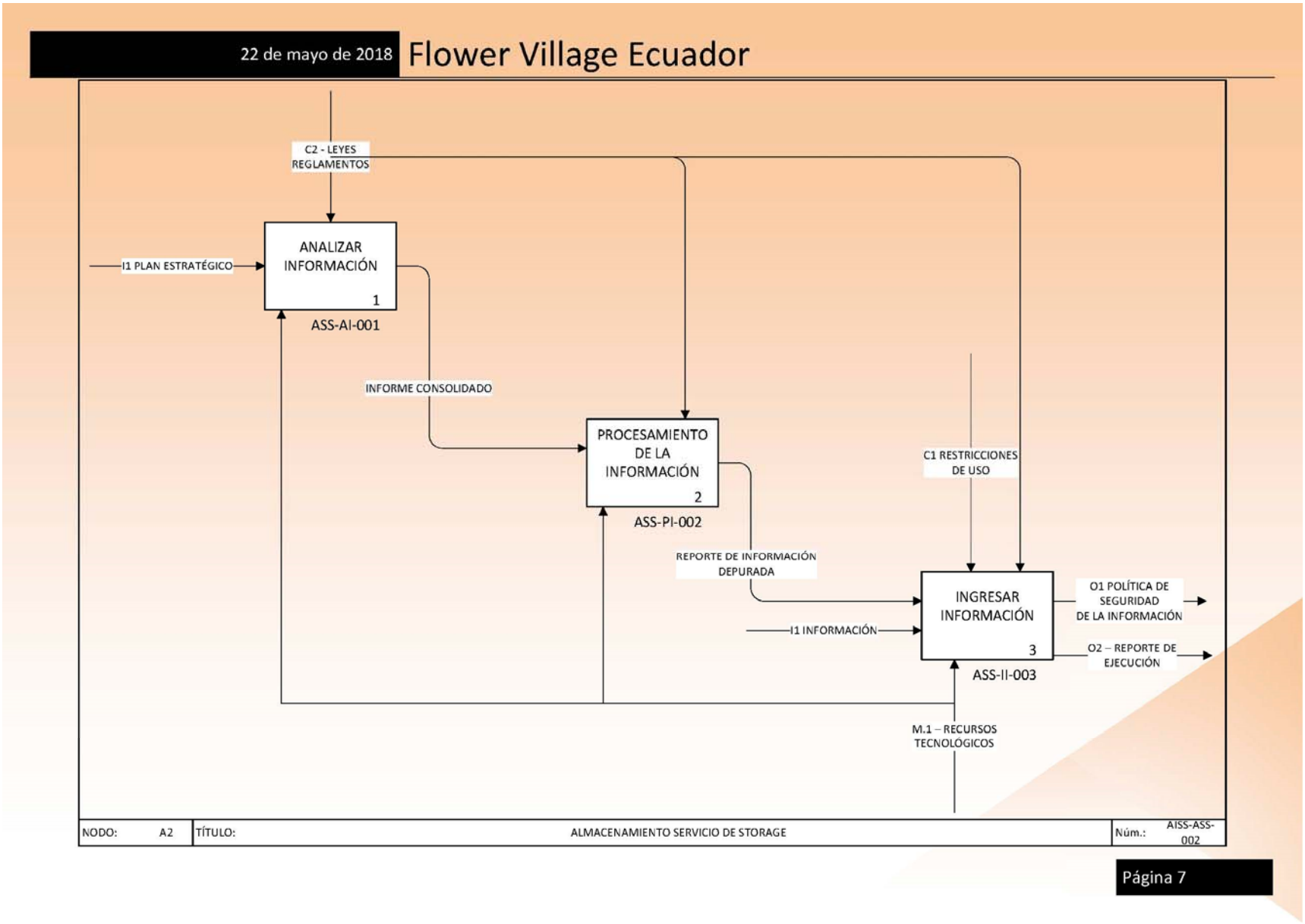

22 de mayo de 2018
Flower Village Ecuador
C2 LEYES REGLAMENTOS
C1 RESTRICCIONES DE USO
EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
1
ESI
PLAN ESTRATÉGICO
I1 INFORMACIÓN
ALMACENAMIENTO SERVICIO DE STORAGE
2
ASS
O1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
M1 RECURSOS TECNOLÓGICOS
REPORTE DE EJECUCIÓN
MEJORAMIENTO CONTINUO
3
MC
INFORME DE MEJORAS
NODO: A0
TÍTULO: ADMINISTRACIÓN DE LA INFORMACIÓN EN EL SERVICIO DE STORAGE
Núm.: AISS -100
Página 2

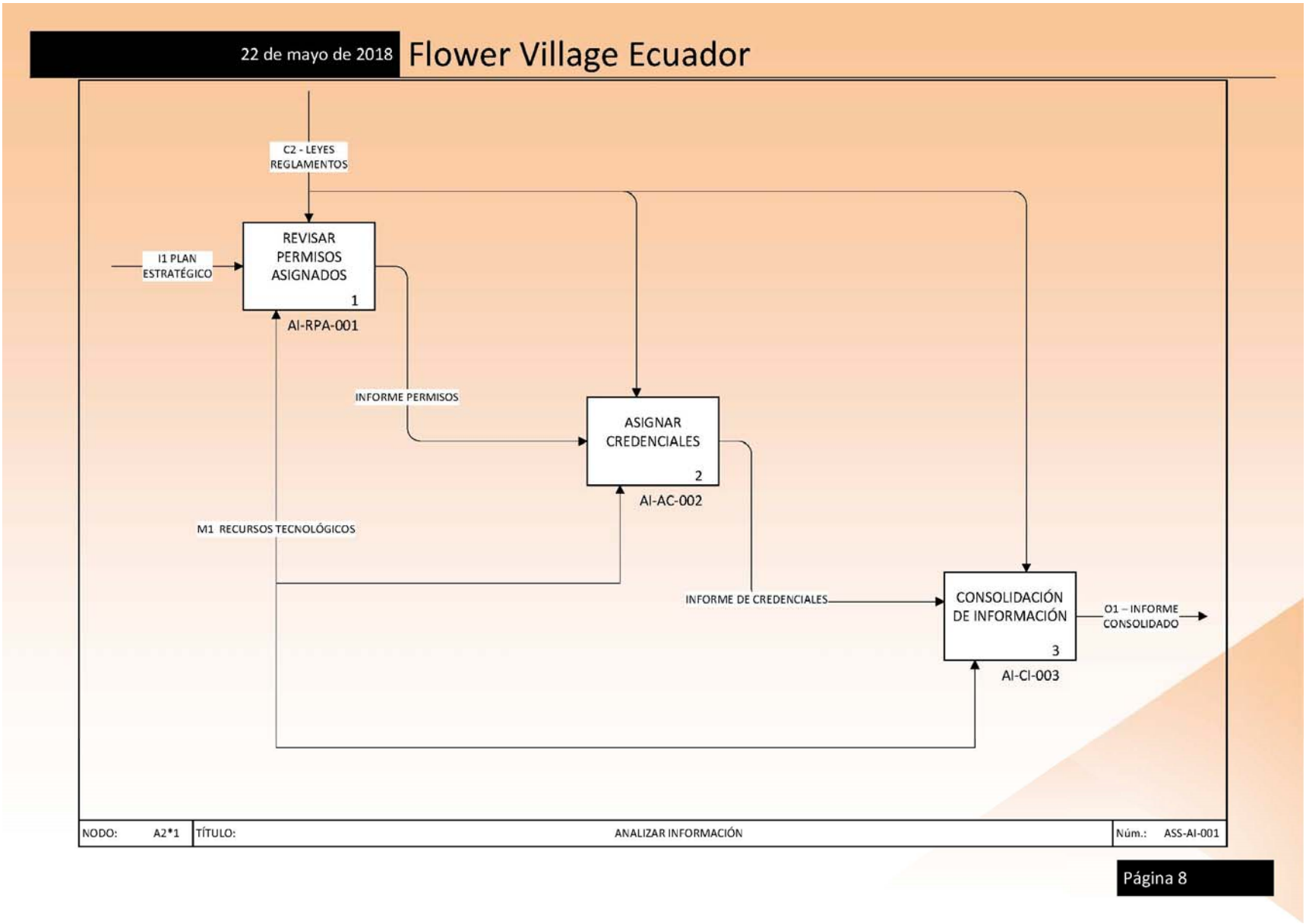

22 de mayo de 2018
Flower Village Ecuador
C2 - LEYES REGLAMENTOS
LEVANTAR INFORMACIÓN
1
ESI-LI-001
INFORMACIÓN DETALLADA
ANALIZAR INFORMACIÓN
2
ESI-AI-002
REPORTE DE INFORMACIÓN
C1 RESTRICCIONES DE USO
M1 RECURSOS TECNOLÓGICOS
ESTABLECER SEGMENTACIÓN
3
ESI-ES-003
O1 PLAN ESTRATÉGICO
NODO: A1
TÍTULO: EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
Núm.: AISS-ESI-001
Página 3

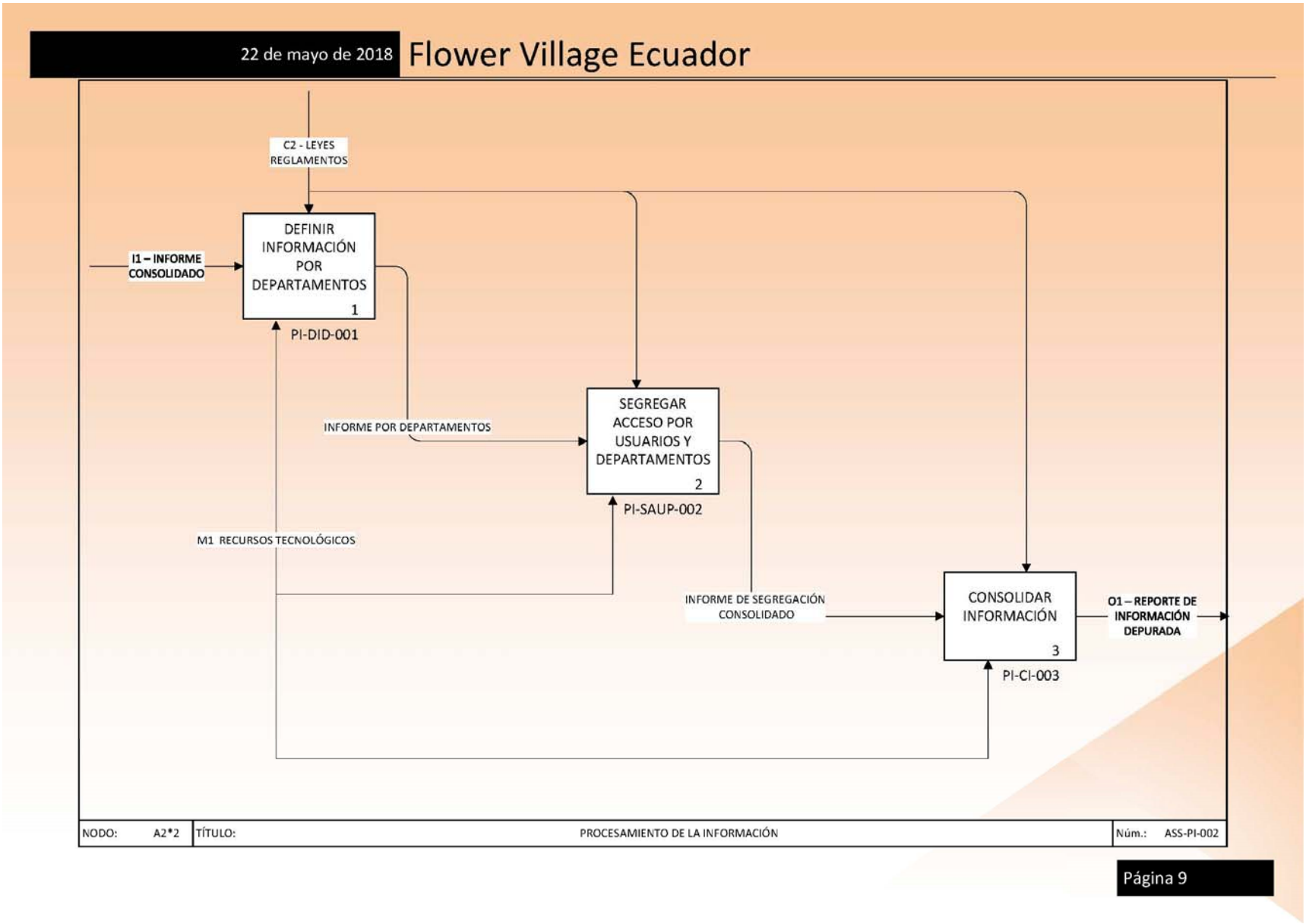

22 de mayo de 2018
Flower Village Ecuador
C2 LEYES REGLAMENTOS
SOLICITAR INFORMACIÓN POR DEPARTAMENTO
1
LI-SID-001
INFORME DE DATOS CONSOLIDADOS
ESTABLECER PARÁMETROS ENTRE DEPARTAMENTOS
2
LI-EPD-001
INFORME PARA REGISTRO DE DATOS
M1 RECURSOS TECNOLÓGICOS
REPORTES CONSOLIDADOS PARA CREAR NORMAS
3
LI-RCCN-001
O1 INFORMACIÓN DETALLADA
NODO: A1*1
TÍTULO: LEVANTAR INFORAMCIÓN
Núm.: ESI-LI-001
Página 4

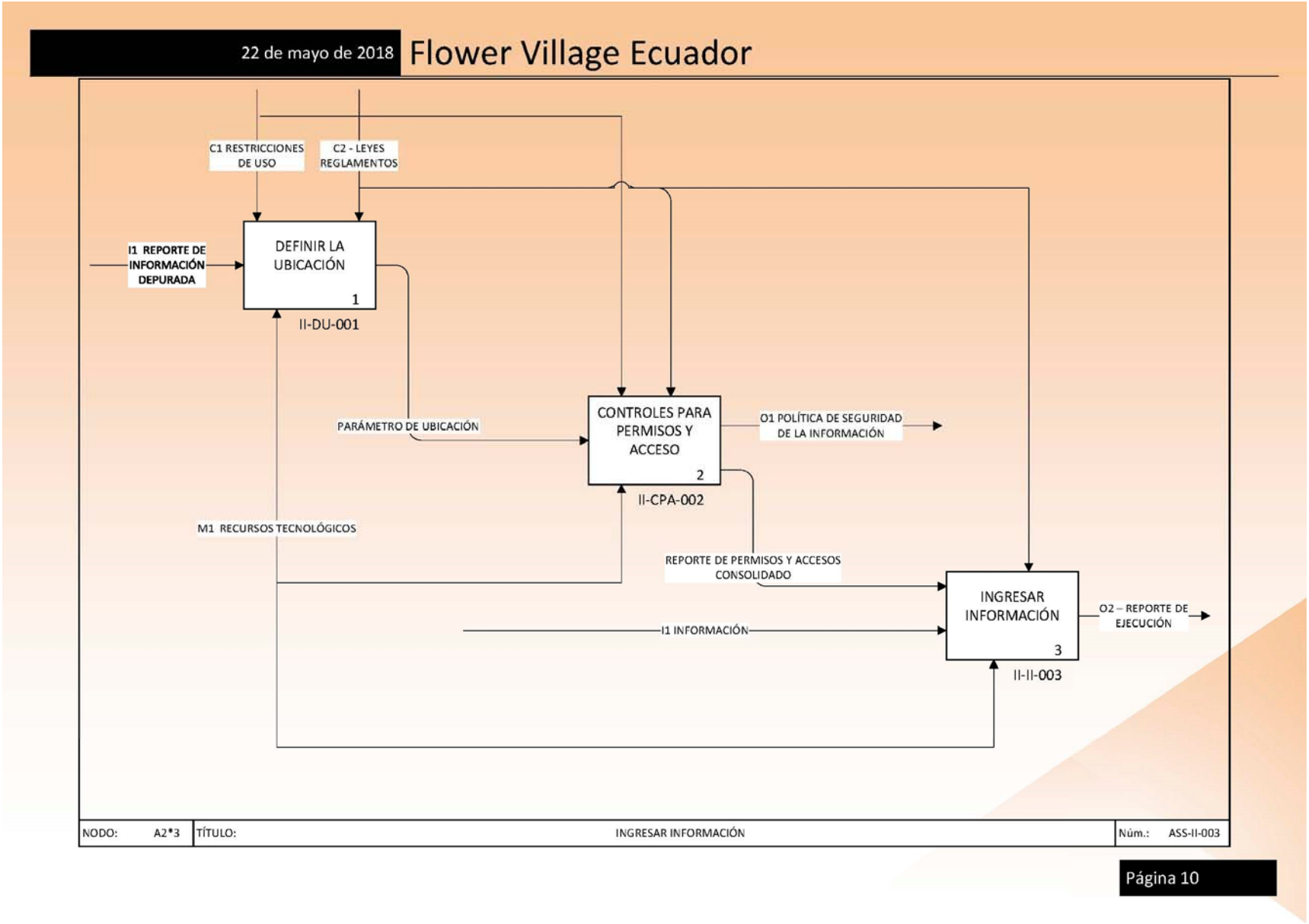

22 de mayo de 2018
Flower Village Ecuador
C2 LEYES REGLAMENTOS
I1 INFORMACIÓN DETALLADA
PROCESAR INFORMACIÓN
1
AI-PI-001
INFORME CON PARAMETROS
CATEGORIZAR INFORMACIÓN
2
AI-CI-002
M1 RECURSOS TECNOLÓGICOS
INFORME CATEGORIZADO
SELECCIONAR INFORMACIÓN
3
AI-SI-001
O1 REPORTE DE INFORMACIÓN
NODO: A1*2
TÍTULO: ANALIZAR INFORMACIÓN
Núm.: ESI-AI-002
Página 5

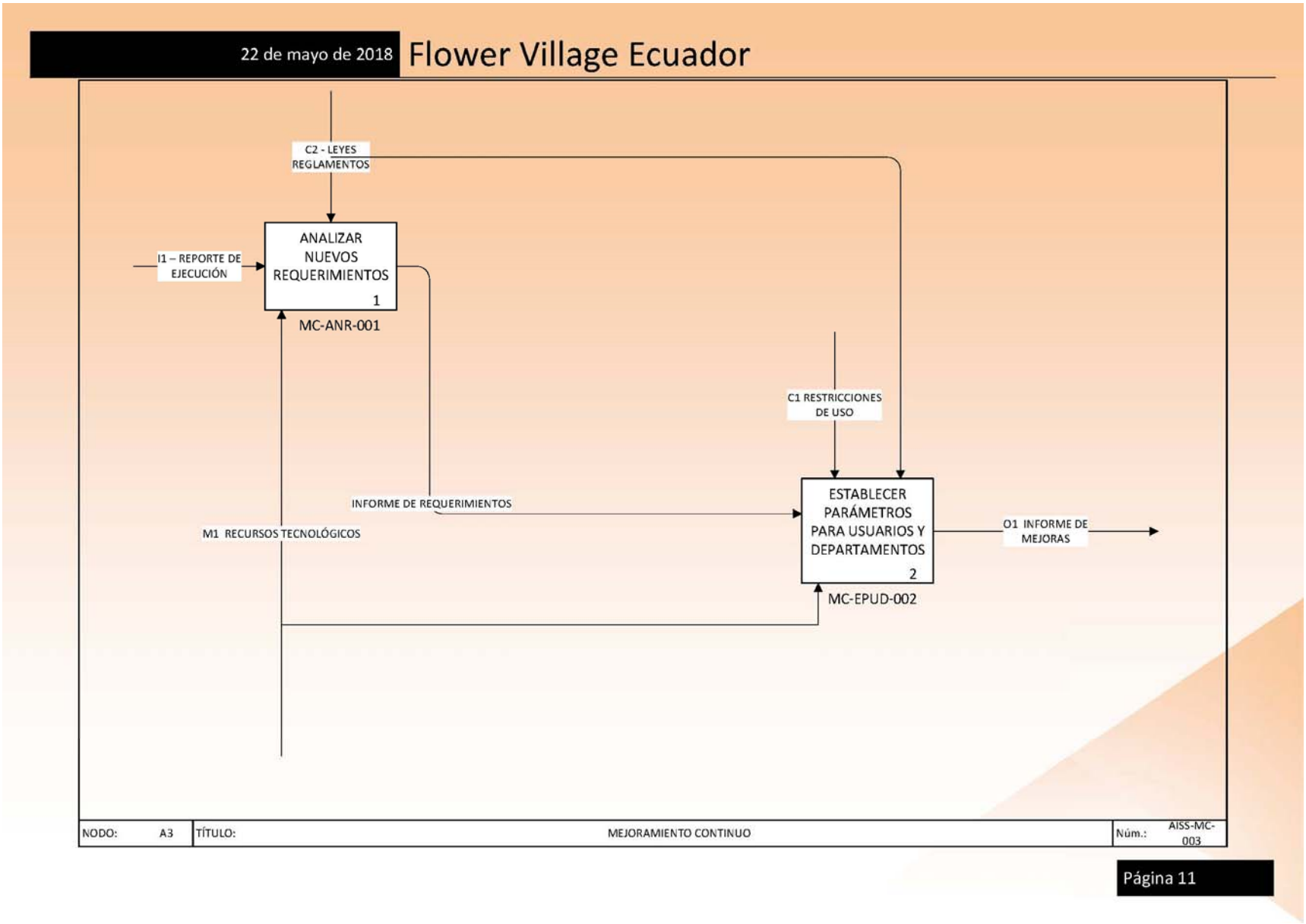

22 de mayo de 2018
Flower Village Ecuador
C1 RESTRICCIONES DE USO
C2 LEYES REGLAMENTOS
I1 REPORTE DE INFORMACIÓN
SEGMENTAR POR DEPARTAMENTO
1
ES-SD-001
REPORTE POR DEPARTAMENTO
SEGMENTAR USUARIOS
2
ES-SU-002
REPORTE DE USUARIOS
M1 RECURSOS TECNOLÓGICOS
SEGMENTAR PERMISOS
3
ES-SP-003
O1 PLAN ESTRATÉGICO
NODO: A1*3
TÍTULO: ESTABLECER SEGMENTACIÓN
Núm.: ESI-ES-003
Página 6

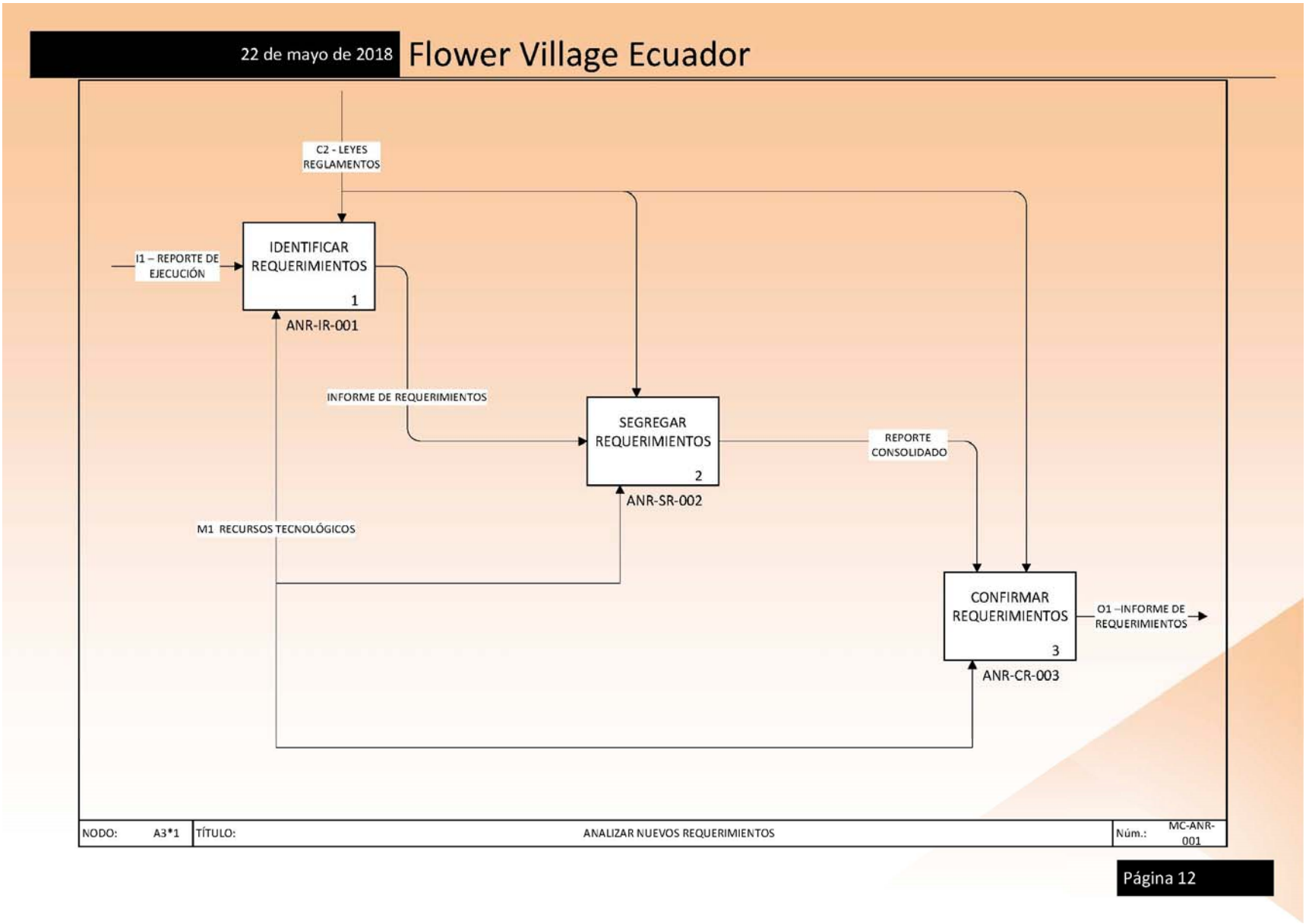

22 de mayo de 2018
Flower Village Ecuador
C2 - LEYES REGLAMENTOS
I1 PLAN ESTRATÉGICO
ANALIZAR INFORMACIÓN
1
ASS-AI-001
INFORME CONSOLIDADO
PROCESAMIENTO DE LA INFORMACIÓN
2
ASS-PI-002
C1 RESTRICCIONES DE USO
REPORTE DE INFORMACIÓN DEPURADA
I1 INFORMACIÓN
INGRESAR INFORMACIÓN
3
ASS-II-003
O1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
O2 – REPORTE DE EJECUCIÓN
M.1 – RECURSOS TECNOLÓGICOS
NODO: A2
TÍTULO: ALMACENAMIENTO SERVICIO DE STORAGE
Núm.: AISS-ASS-002
Página 7

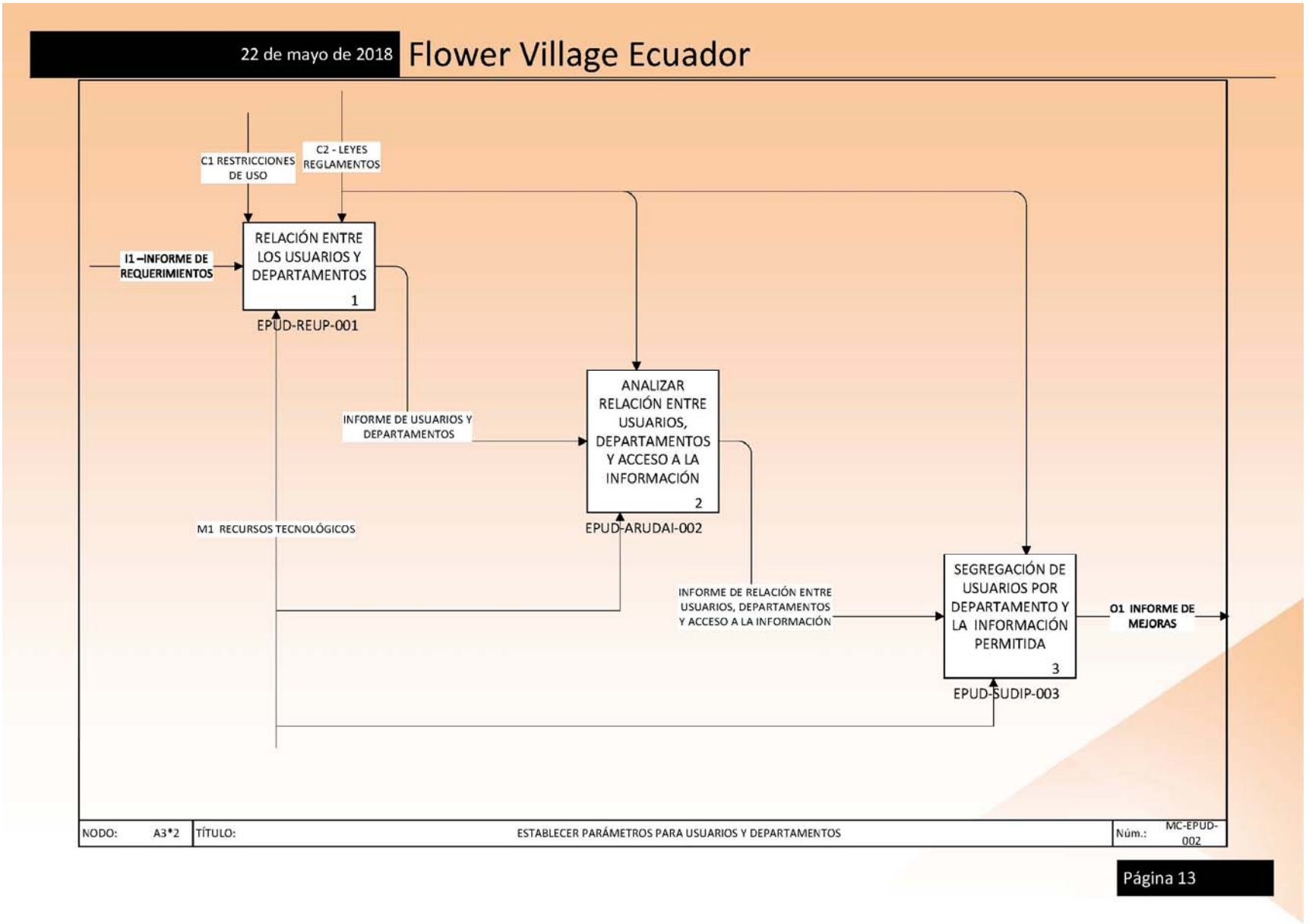

22 de mayo de 2018
Flower Village Ecuador
C2 - LEYES REGLAMENTOS
I1 PLAN ESTRATÉGICO
REVISAR PERMISOS ASIGNADOS
1
AI-RPA-001
INFORME PERMISOS
ASIGNAR CREDENCIALES
2
AI-AC-002
M1 RECURSOS TECNOLÓGICOS
INFORME DE CREDENCIALES
CONSOLIDACIÓN DE INFORMACIÓN
3
AI-CI-003
O1 – INFORME CONSOLIDADO
NODO: A2*1
TÍTULO: ANALIZAR INFORMACIÓN
Núm.: ASS-AI-001
Página 8

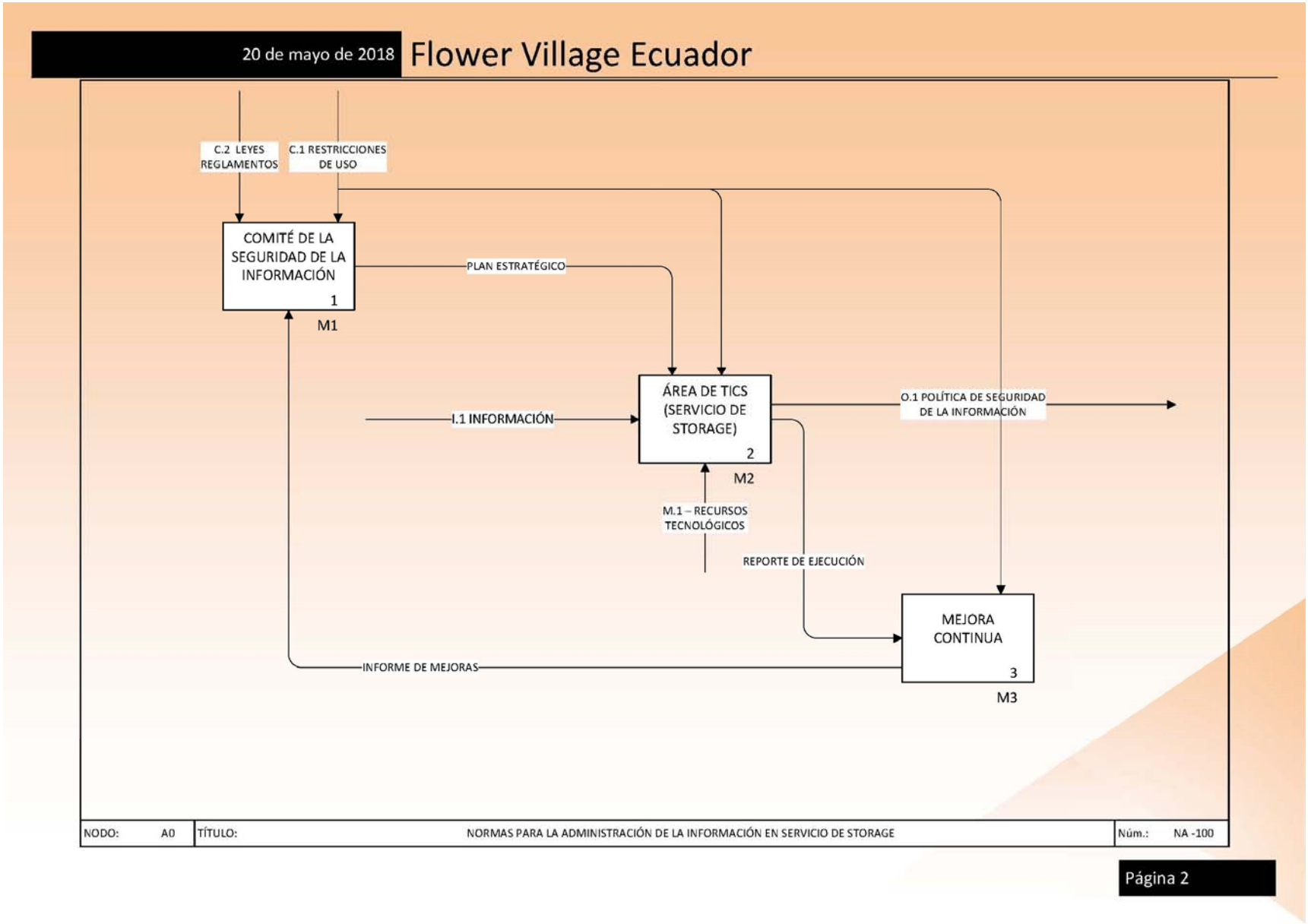

22 de mayo de 2018
Flower Village Ecuador
C2 - LEYES REGLAMENTOS
I1 – INFORME CONSOLIDADO
DEFINIR INFORMACIÓN POR DEPARTAMENTOS
1
PI-DID-001
INFORME POR DEPARTAMENTOS
SEGREGAR ACCESO POR USUARIOS Y DEPARTAMENTOS
2
PI-SAUP-002
M1 RECURSOS TECNOLÓGICOS
INFORME DE SEGREGACIÓN CONSOLIDADO
CONSOLIDAR INFORMACIÓN
3
PI-CI-003
O1 – REPORTE DE INFORMACIÓN DEPURADA
NODO: A2*2
TÍTULO: PROCESAMIENTO DE LA INFORMACIÓN
Núm.: ASS-PI-002
Página 9

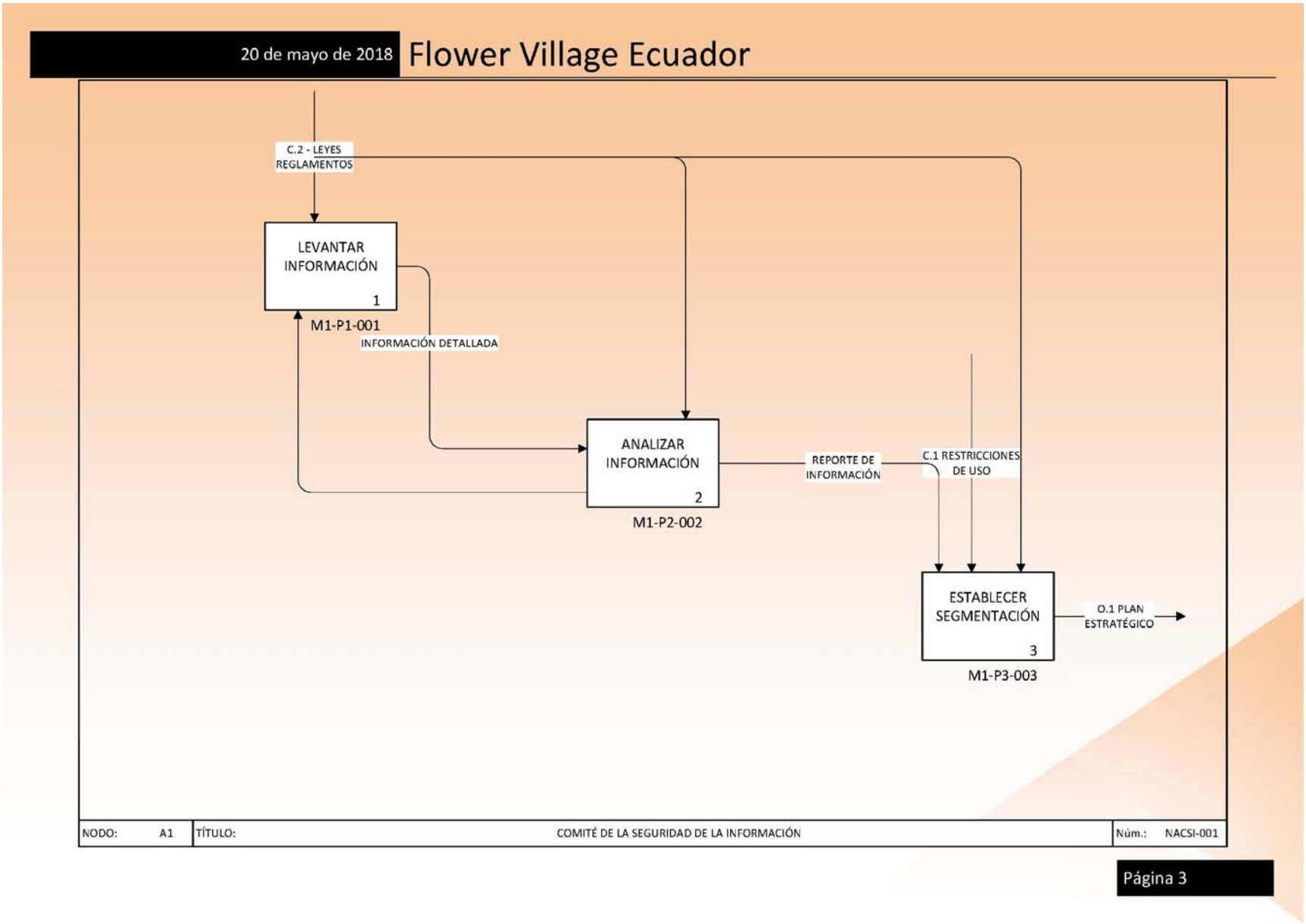

22 de mayo de 2018
Flower Village Ecuador
C1 RESTRICCIONES DE USO
C2 - LEYES REGLAMENTOS
I1 REPORTE DE INFORMACIÓN DEPURADA
DEFINIR LA UBICACIÓN
1
II-DU-001
PARÁMETRO DE UBICACIÓN
CONTROLES PARA PERMISOS Y ACCESO
2
II-CPA-002
O1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
M1 RECURSOS TECNOLÓGICOS
REPORTE DE PERMISOS Y ACCESOS CONSOLIDADO
INGRESAR INFORMACIÓN
3
II-II-003
I1 INFORMACIÓN
O2 – REPORTE DE EJECUCIÓN
NODO: A2*3
TÍTULO: INGRESAR INFORMACIÓN
Núm.: ASS-II-003
Página 10

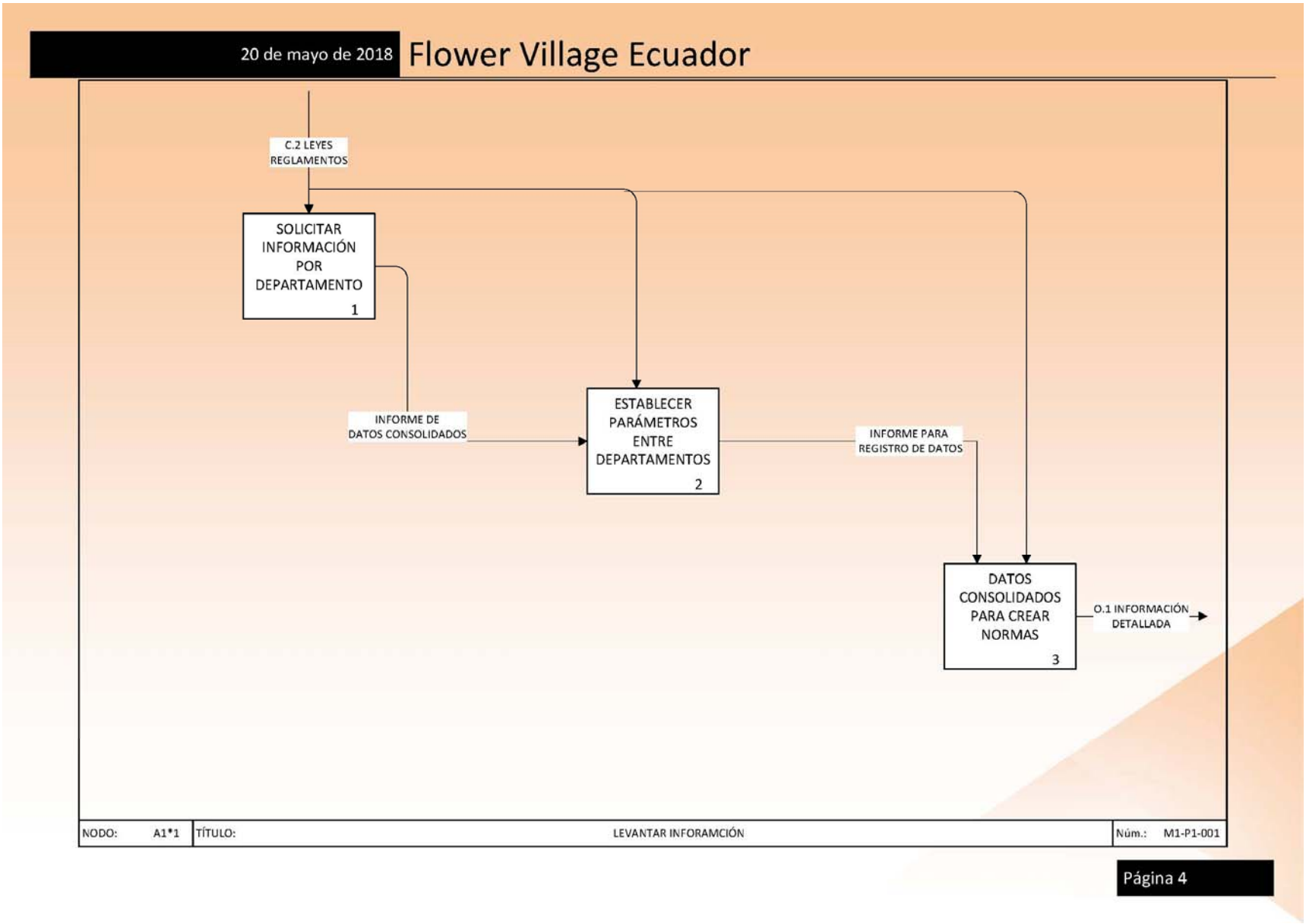

22 de mayo de 2018
Flower Village Ecuador
C2 - LEYES REGLAMENTOS
I1 – REPORTE DE EJECUCIÓN
ANALIZAR NUEVOS REQUERIMIENTOS
1
MC-ANR-001
C1 RESTRICCIONES DE USO
INFORME DE REQUERIMIENTOS
M1 RECURSOS TECNOLÓGICOS
ESTABLECER PARÁMETROS PARA USUARIOS Y DEPARTAMENTOS
2
MC-EPUD-002
O1 INFORME DE MEJORAS
NODO: A3
TÍTULO: MEJORAMIENTO CONTINUO
Núm.: AISS-MC-003
Página 11

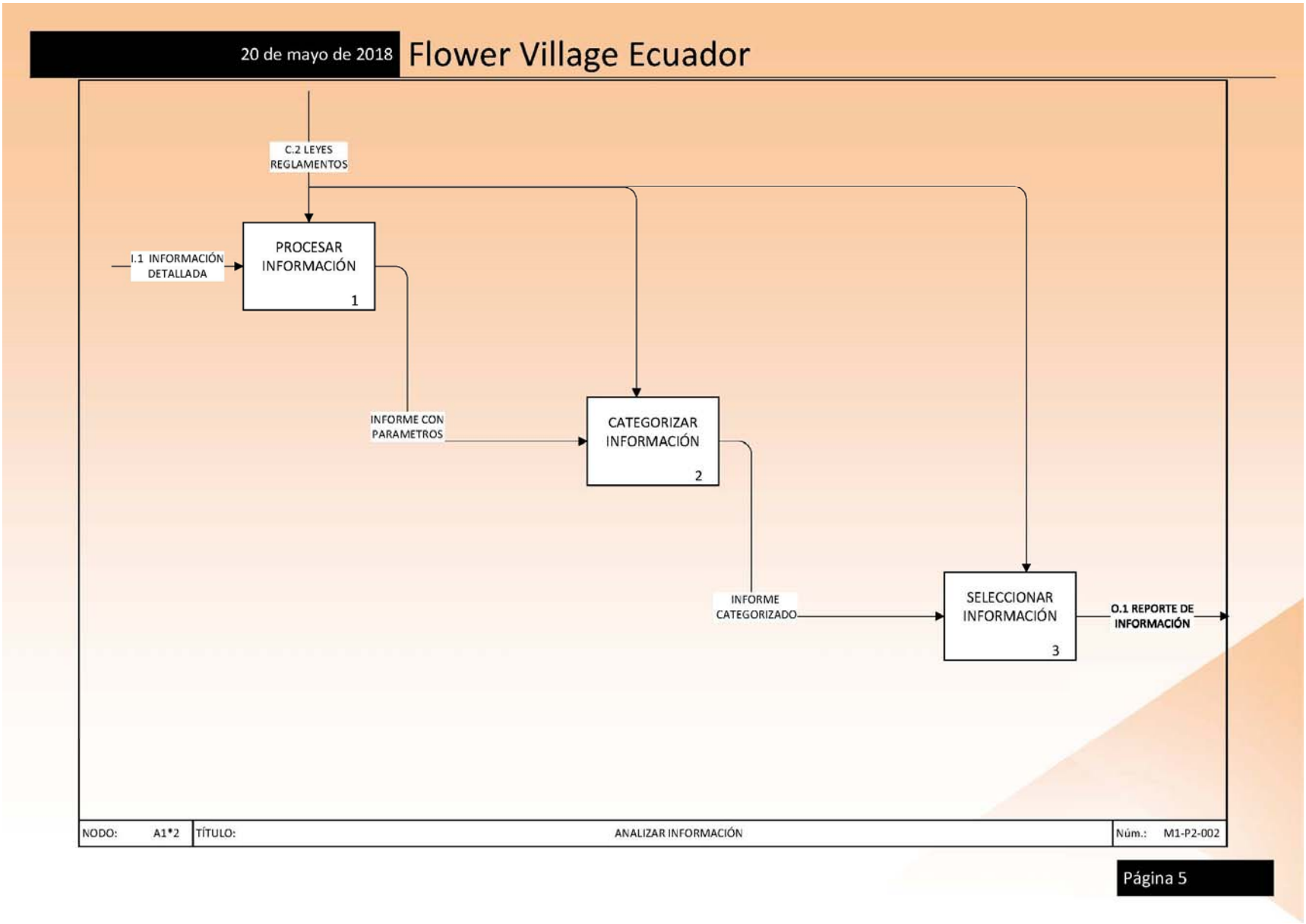

22 de mayo de 2018
Flower Village Ecuador
C2 - LEYES REGLAMENTOS
I1 – REPORTE DE EJECUCIÓN
IDENTIFICAR REQUERIMIENTOS
1
ANR-IR-001
INFORME DE REQUERIMIENTOS
SEGREGAR REQUERIMIENTOS
2
ANR-SR-002
REPORTE CONSOLIDADO
M1 RECURSOS TECNOLÓGICOS
CONFIRMAR REQUERIMIENTOS
3
ANR-CR-003
O1 –INFORME DE REQUERIMIENTOS
NODO: A3*1
TÍTULO: ANALIZAR NUEVOS REQUERIMIENTOS
Núm.: MC-ANR-001
Página 12

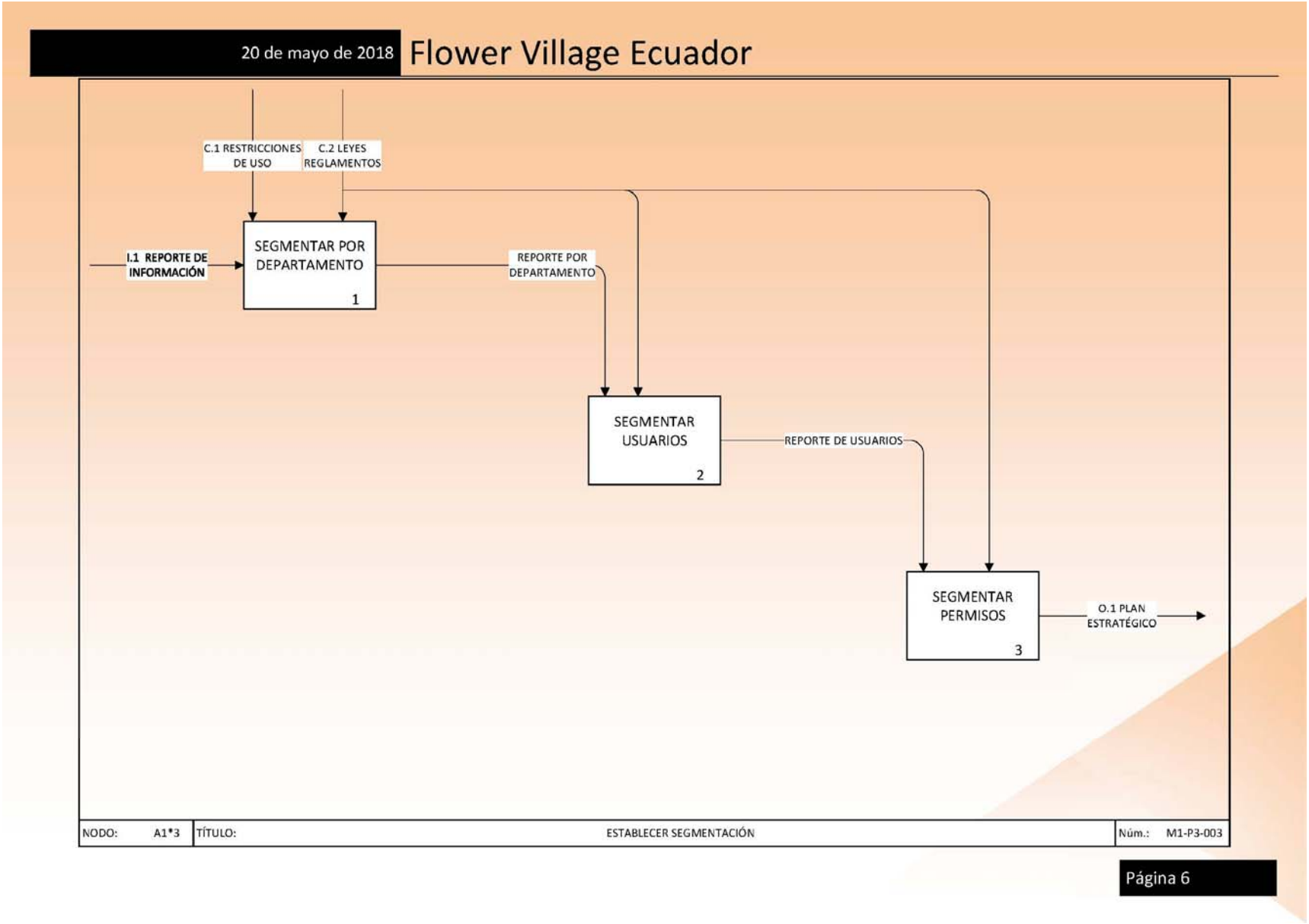

22 de mayo de 2018
Flower Village Ecuador
C1 RESTRICCIONES DE USO
C2 - LEYES REGLAMENTOS
I1 –INFORME DE REQUERIMIENTOS
RELACIÓN ENTRE LOS USUARIOS Y DEPARTAMENTOS
1
EPUD-REUP-001
INFORME DE USUARIOS Y DEPARTAMENTOS
ANALIZAR RELACIÓN ENTRE USUARIOS, DEPARTAMENTOS Y ACCESO A LA INFORMACIÓN
2
EPUD-ARUDAI-002
M1 RECURSOS TECNOLÓGICOS
INFORME DE RELACIÓN ENTRE USUARIOS, DEPARTAMENTOS Y ACCESO A LA INFORMACIÓN
SEGREGACIÓN DE USUARIOS POR DEPARTAMENTO Y LA INFORMACIÓN PERMITIDA
3
EPUD-SUDIP-003
O1 INFORME DE MEJORAS
NODO: A3*2
TÍTULO: ESTABLECER PARÁMETROS PARA USUARIOS Y DEPARTAMENTOS
Núm.: MC-EPUD-002
Página 13

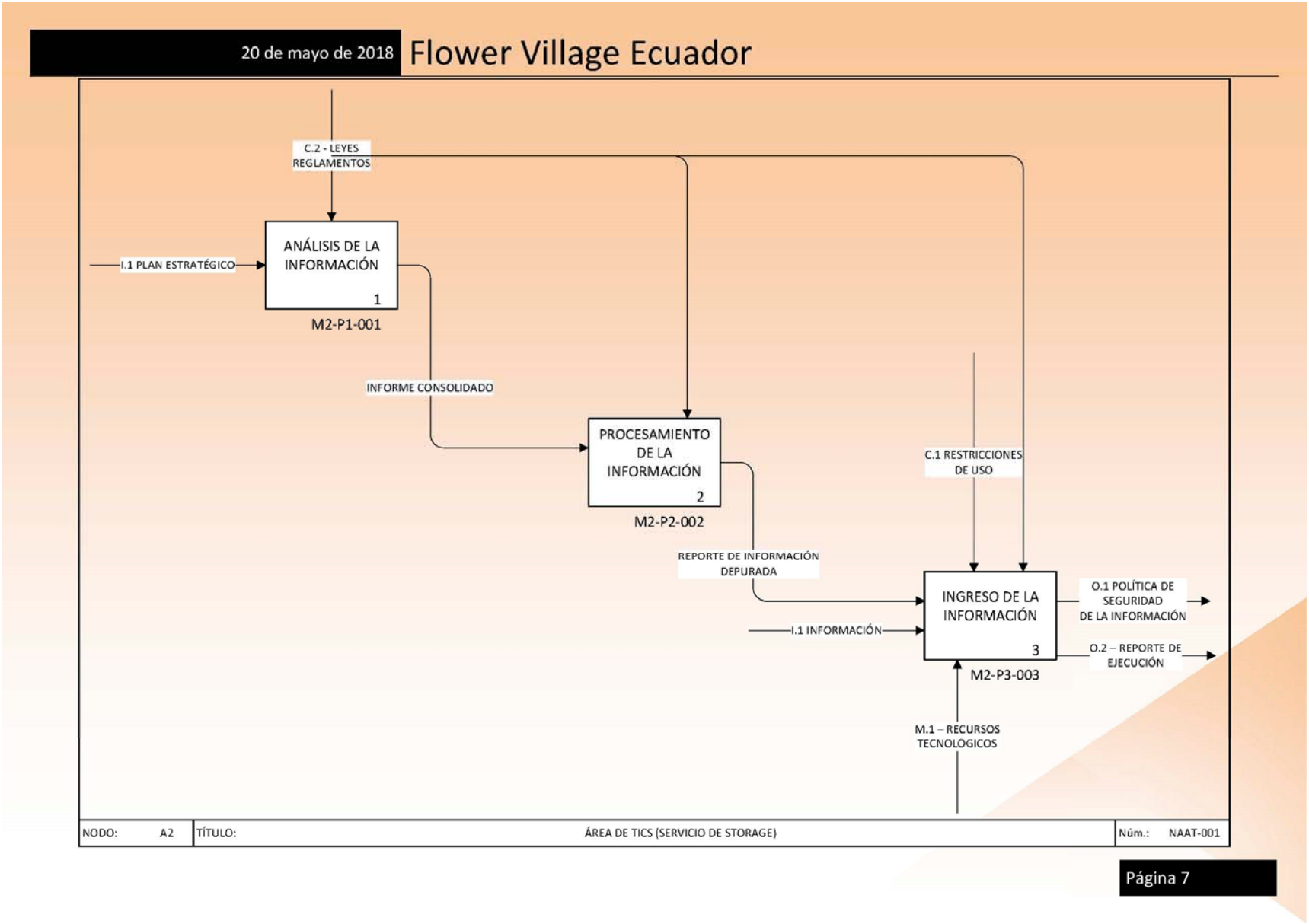

20 de mayo de 2018
Flower Village Ecuador
C.2 LEYES REGLAMENTOS
C.1 RESTRICCIONES DE USO
COMITÉ DE LA SEGURIDAD DE LA INFORMACIÓN
1
M1
PLAN ESTRATÉGICO
ÁREA DE TICS (SERVICIO DE STORAGE)
2
M2
I.1 INFORMACIÓN
O.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
M.1 – RECURSOS TECNOLÓGICOS
REPORTE DE EJECUCIÓN
MEJORA CONTINUA
3
M3
INFORME DE MEJORAS
NODO: A0
TÍTULO: NORMAS PARA LA ADMINISTRACIÓN DE LA INFORMACIÓN EN SERVICIO DE STORAGE
Núm.: NA -100
Página 2

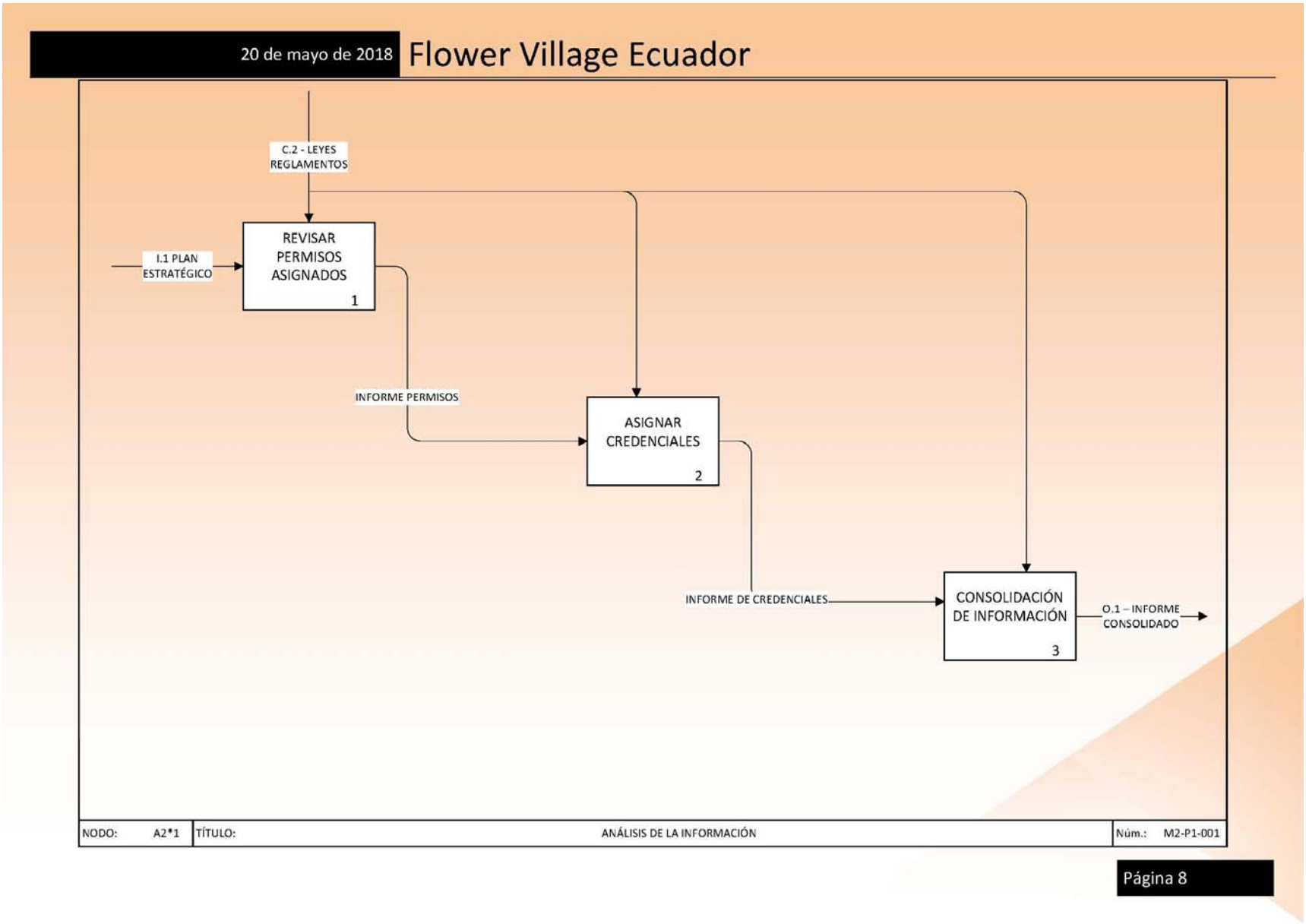

20 de mayo de 2018
Flower Village Ecuador
C.2 - LEYES REGLAMENTOS
LEVANTAR INFORMACIÓN
1
M1-P1-001
INFORMACIÓN DETALLADA
ANALIZAR INFORMACIÓN
2
M1-P2-002
REPORTE DE INFORMACIÓN
C.1 RESTRICCIONES DE USO
ESTABLECER SEGMENTACIÓN
3
M1-P3-003
O.1 PLAN ESTRATÉGICO
NODO: A1
TÍTULO: COMITÉ DE LA SEGURIDAD DE LA INFORMACIÓN
Núm.: NACSI-001
Página 3

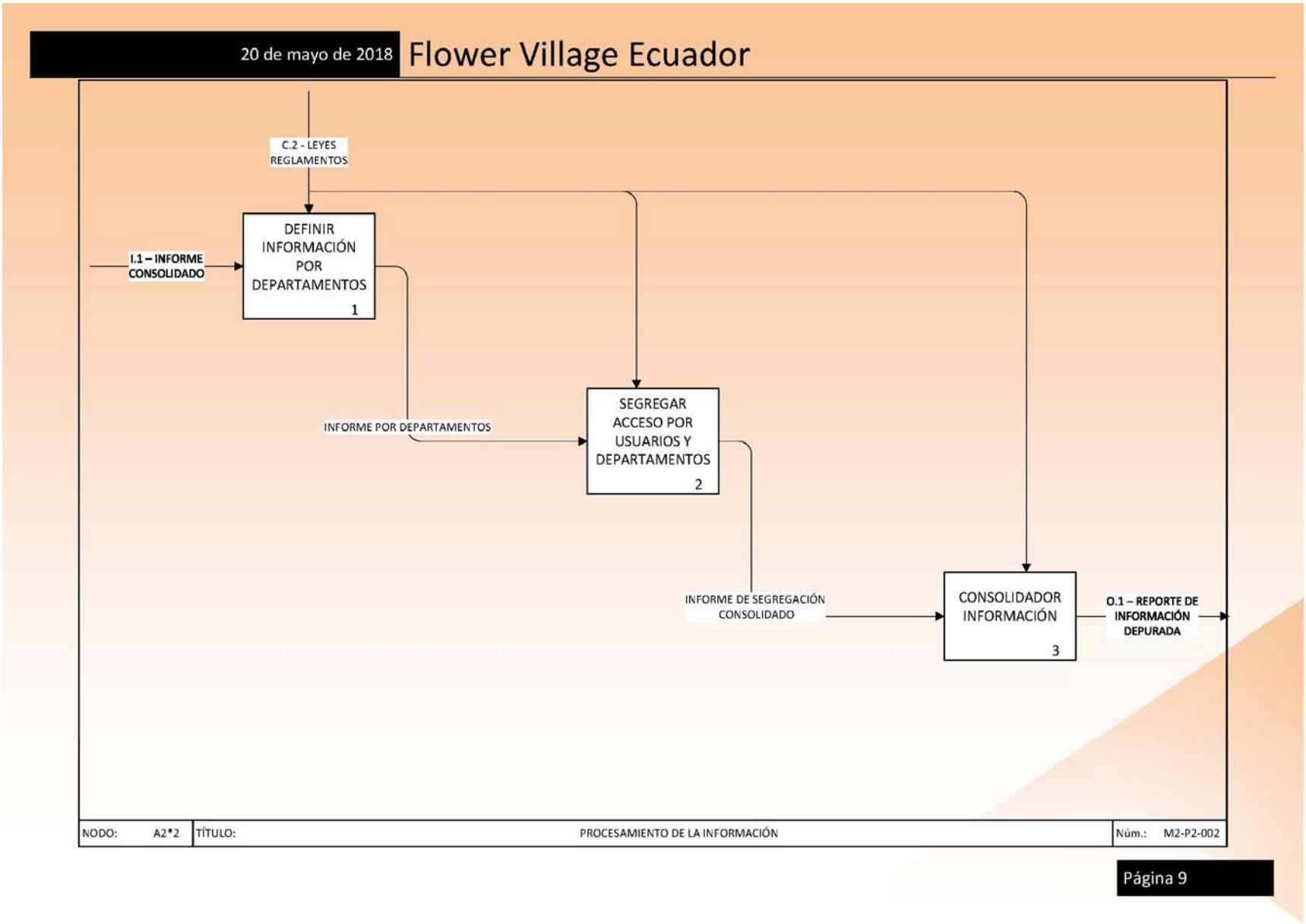

20 de mayo de 2018
Flower Village Ecuador
C.2 LEYES REGLAMENTOS
SOLICITAR INFORMACIÓN POR DEPARTAMENTO
1
INFORME DE DATOS CONSOLIDADOS
ESTABLECER PARÁMETROS ENTRE DEPARTAMENTOS
2
INFORME PARA REGISTRO DE DATOS
DATOS CONSOLIDADOS PARA CREAR NORMAS
3
O.1 INFORMACIÓN DETALLADA
NODO: A1*1
TÍTULO: LEVANTAR INFORAMCIÓN
Núm.: M1-P1-001
Página 4

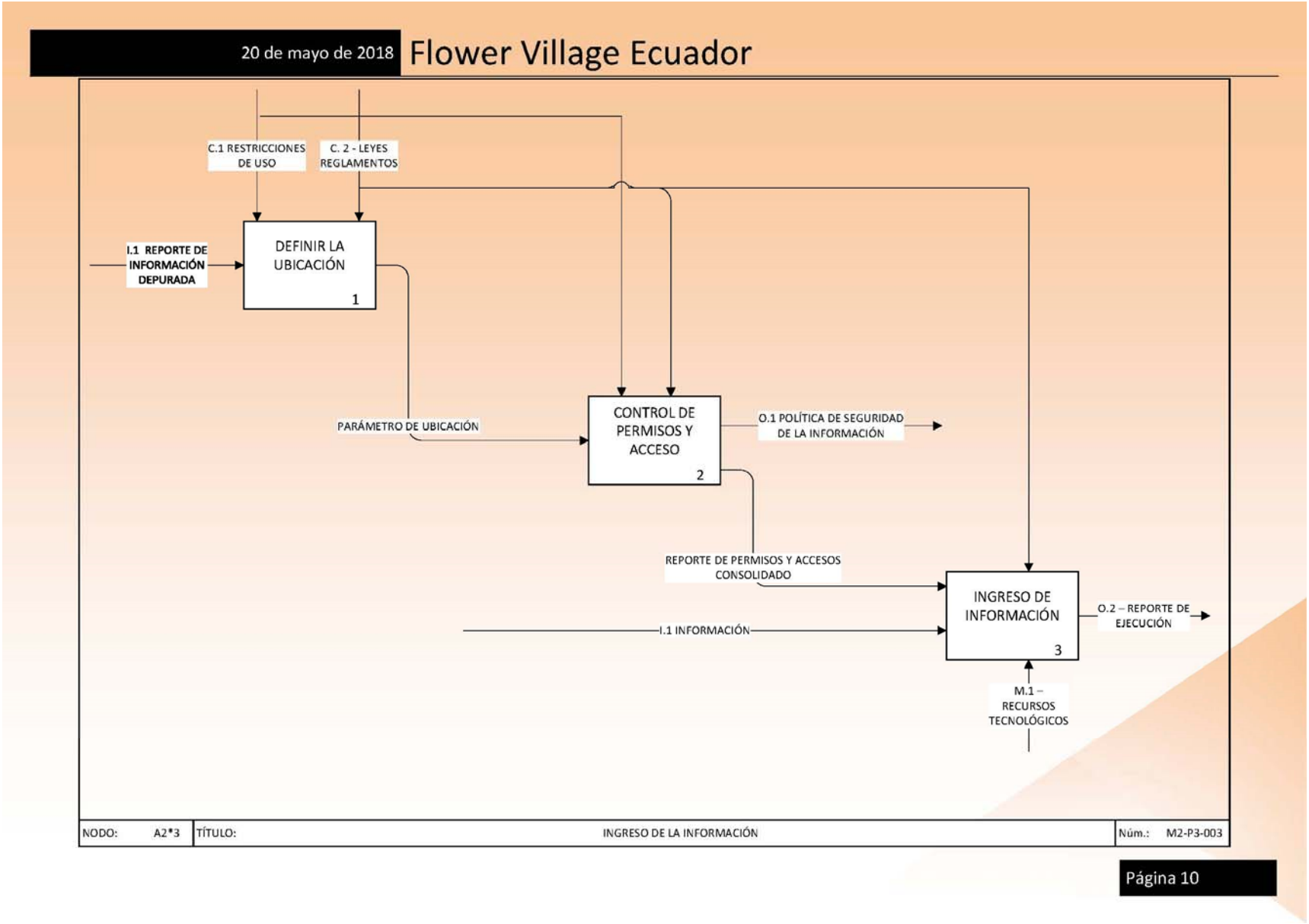

20 de mayo de 2018
Flower Village Ecuador
C.2 LEYES REGLAMENTOS
I.1 INFORMACIÓN DETALLADA
PROCESAR INFORMACIÓN
1
INFORME CON PARAMETROS
CATEGORIZAR INFORMACIÓN
2
INFORME CATEGORIZADO
SELECCIONAR INFORMACIÓN
3
O.1 REPORTE DE INFORMACIÓN
NODO: A1*2
TÍTULO: ANALIZAR INFORMACIÓN
Núm.: M1-P2-002
Página 5

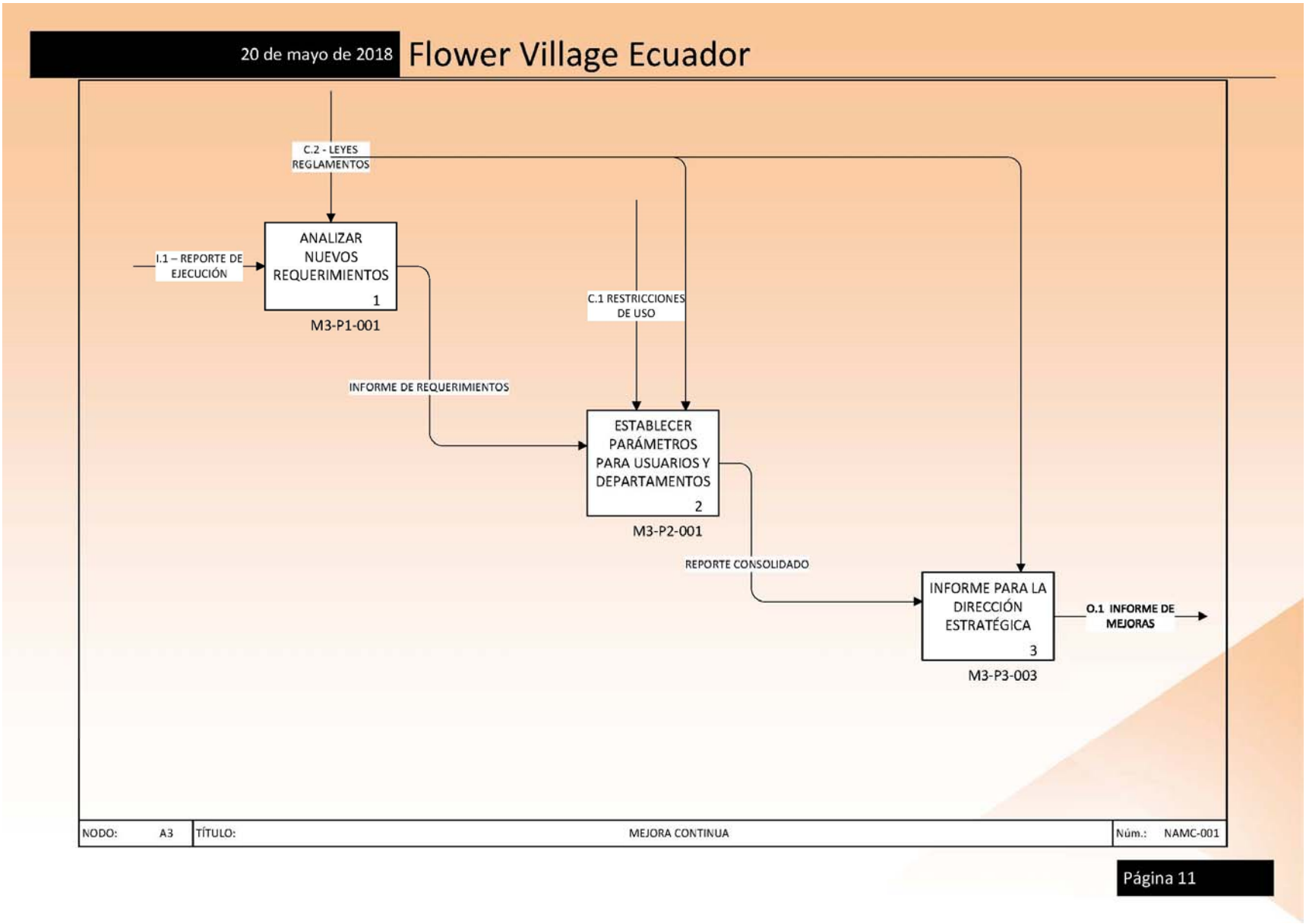

20 de mayo de 2018
Flower Village Ecuador
C.1 RESTRICCIONES DE USO
C.2 LEYES REGLAMENTOS
I.1 REPORTE DE INFORMACIÓN
SEGMENTAR POR DEPARTAMENTO
1
REPORTE POR DEPARTAMENTO
SEGMENTAR USUARIOS
2
REPORTE DE USUARIOS
SEGMENTAR PERMISOS
3
O.1 PLAN ESTRATÉGICO
NODO: A1*3
TÍTULO:
ESTABLECER SEGMENTACIÓN
Núm.: M1-P3-003
Página 6

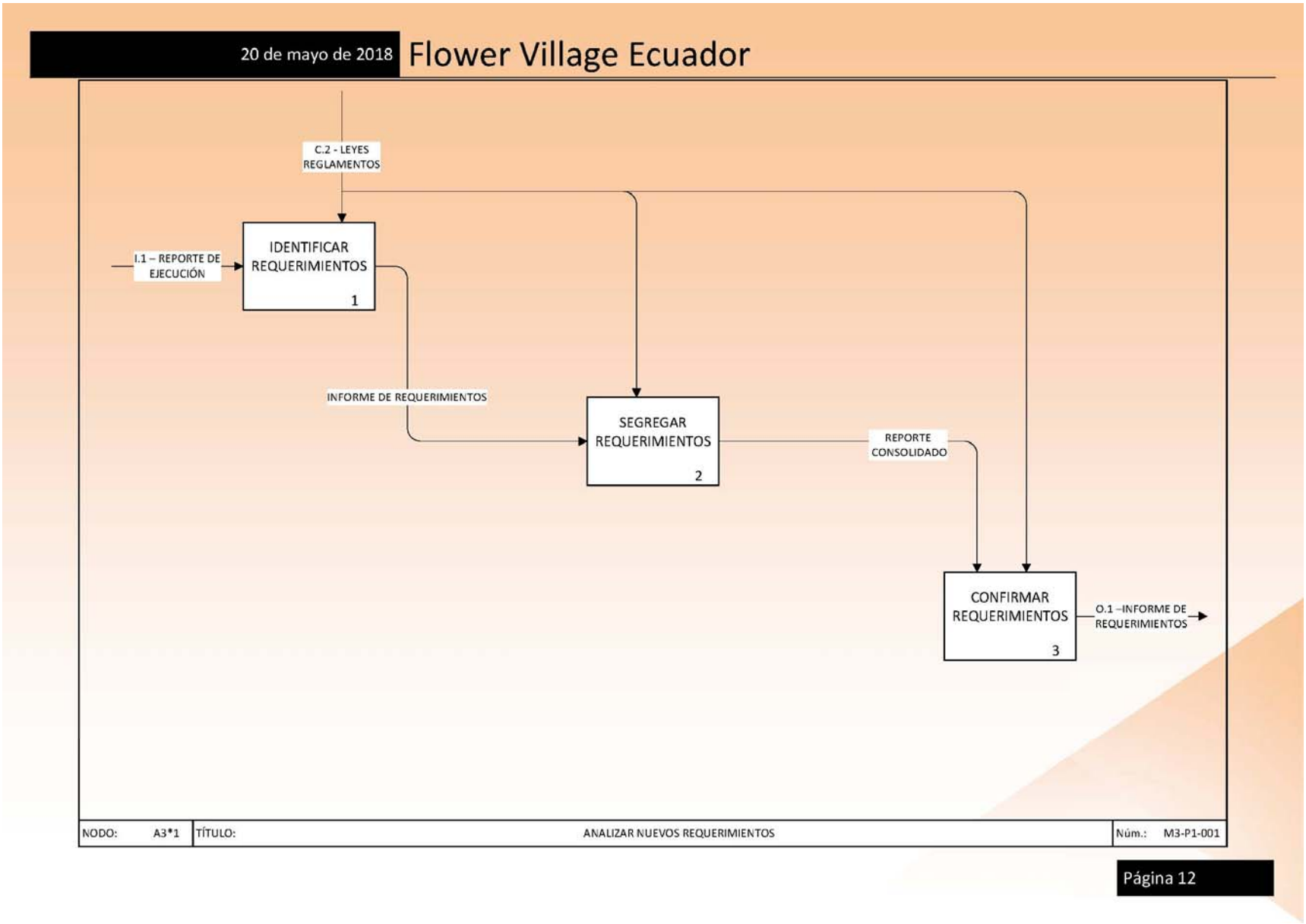

20 de mayo de 2018
Flower Village Ecuador
C.2 - LEYES REGLAMENTOS
I.1 PLAN ESTRATÉGICO
ANÁLISIS DE LA INFORMACIÓN
1
M2-P1-001
INFORME CONSOLIDADO
PROCESAMIENTO DE LA INFORMACIÓN
2
M2-P2-002
C.1 RESTRICCIONES DE USO
REPORTE DE INFORMACIÓN DEPURADA
I.1 INFORMACIÓN
INGRESO DE LA INFORMACIÓN
3
M2-P3-003
O.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
O.2 – REPORTE DE EJECUCIÓN
M.1 – RECURSOS TECNOLÓGICOS
NODO: A2
TÍTULO: ÁREA DE TICS (SERVICIO DE STORAGE)
Núm.: NAAT-001
Página 7

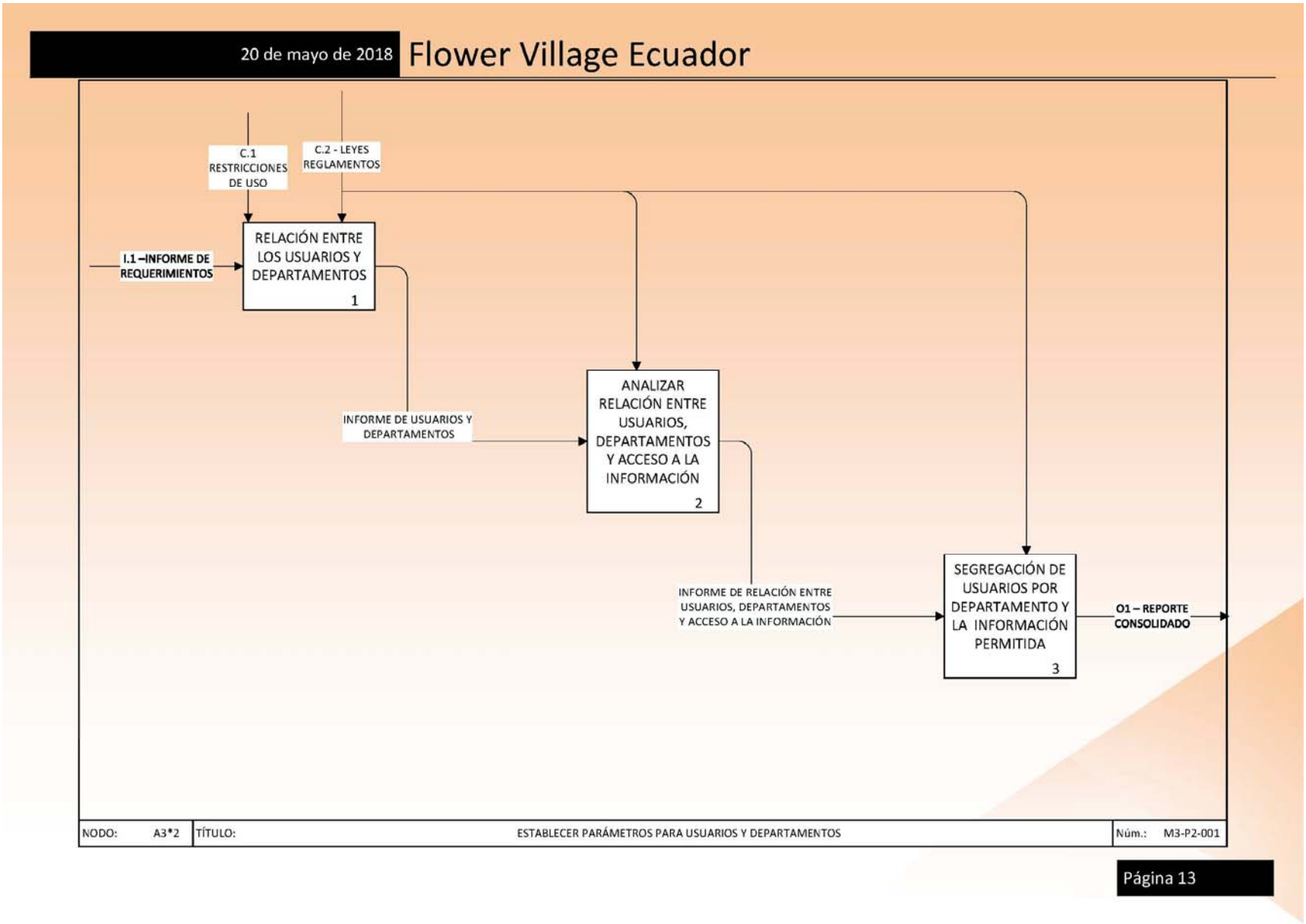

20 de mayo de 2018
Flower Village Ecuador
C.2 - LEYES REGLAMENTOS
I.1 PLAN ESTRATÉGICO
REVISAR PERMISOS ASIGNADOS
1
INFORME PERMISOS
ASIGNAR CREDENCIALES
2
INFORME DE CREDENCIALES
CONSOLIDACIÓN DE INFORMACIÓN
3
O.1 – INFORME CONSOLIDADO
NODO: A2*1
TÍTULO:
ANÁLISIS DE LA INFORMACIÓN
Núm.: M2-P1-001
Página 8

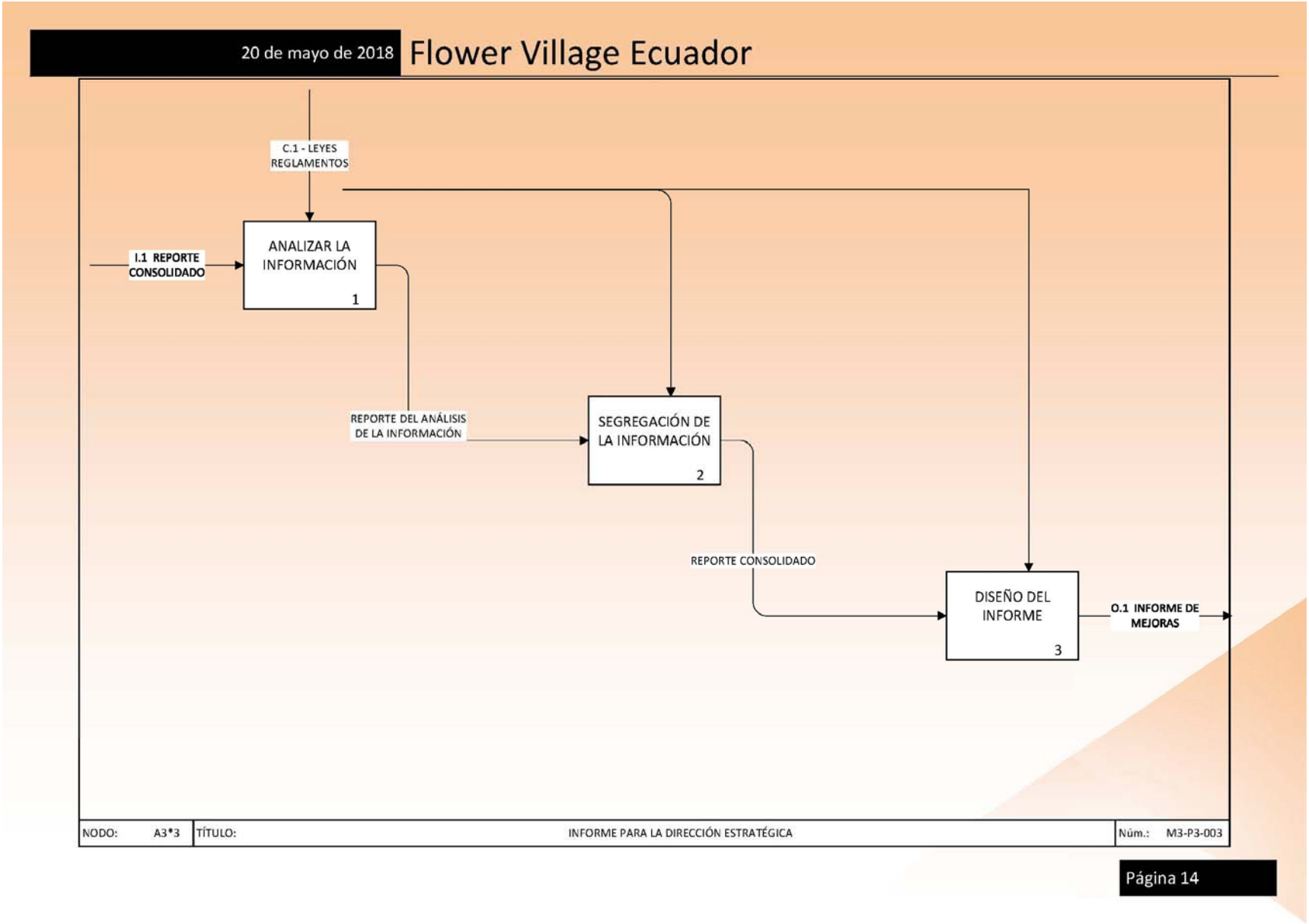

20 de mayo de 2018
Flower Village Ecuador
C.2 - LEYES REGLAMENTOS
I.1 – INFORME CONSOLIDADO
DEFINIR INFORMACIÓN POR DEPARTAMENTOS
1
INFORME POR DEPARTAMENTOS
SEGREGAR ACCESO POR USUARIOS Y DEPARTAMENTOS
2
INFORME DE SEGREGACIÓN CONSOLIDADO
CONSOLIDADOR INFORMACIÓN
3
O.1 – REPORTE DE INFORMACIÓN DEPURADA
NODO: A2*2
TÍTULO: PROCESAMIENTO DE LA INFORMACIÓN
Núm.: M2-P2-002
Página 9


20 de mayo de 2018
Flower Village Ecuador
C.1 RESTRICCIONES DE USO
C. 2 - LEYES REGLAMENTOS
I.1 REPORTE DE INFORMACIÓN DEPURADA
DEFINIR LA UBICACIÓN
1
PARÁMETRO DE UBICACIÓN
CONTROL DE PERMISOS Y ACCESO
2
O.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
REPORTE DE PERMISOS Y ACCESOS CONSOLIDADO
I.1 INFORMACIÓN
INGRESO DE INFORMACIÓN
3
O.2 – REPORTE DE EJECUCIÓN
M.1 – RECURSOS TECNOLÓGICOS
NODO: A2*3
TÍTULO: INGRESO DE LA INFORMACIÓN
Núm.: M2-P3-003
Página 10


20 de mayo de 2018
Flower Village Ecuador
C.2 - LEYES REGLAMENTOS
I.1 – REPORTE DE EJECUCIÓN
ANALIZAR NUEVOS REQUERIMIENTOS
1
M3-P1-001
C.1 RESTRICCIONES DE USO
INFORME DE REQUERIMIENTOS
ESTABLECER PARÁMETROS PARA USUARIOS Y DEPARTAMENTOS
2
M3-P2-001
REPORTE CONSOLIDADO
INFORME PARA LA DIRECCIÓN ESTRATÉGICA
3
M3-P3-003
O.1 INFORME DE MEJORAS
NODO: A3
TÍTULO: MEJORA CONTINUA
Núm.: NAMC-001
Página 11


20 de mayo de 2018
Flower Village Ecuador
C.2 - LEYES REGLAMENTOS
I.1 – REPORTE DE EJECUCIÓN
IDENTIFICAR REQUERIMIENTOS
1
INFORME DE REQUERIMIENTOS
SEGREGAR REQUERIMIENTOS
2
REPORTE CONSOLIDADO
CONFIRMAR REQUERIMIENTOS
3
O.1 –INFORME DE REQUERIMIENTOS
NODO: A3*1
TÍTULO: ANALIZAR NUEVOS REQUERIMIENTOS
Núm.: M3-P1-001
Página 12


20 de mayo de 2018
Flower Village Ecuador
C.1 RESTRICCIONES DE USO
C.2 - LEYES REGLAMENTOS
I.1 –INFORME DE REQUERIMIENTOS
RELACIÓN ENTRE LOS USUARIOS Y DEPARTAMENTOS
1
INFORME DE USUARIOS Y DEPARTAMENTOS
ANALIZAR RELACIÓN ENTRE USUARIOS, DEPARTAMENTOS Y ACCESO A LA INFORMACIÓN
2
INFORME DE RELACIÓN ENTRE USUARIOS, DEPARTAMENTOS Y ACCESO A LA INFORMACIÓN
SEGREGACIÓN DE USUARIOS POR DEPARTAMENTO Y LA INFORMACIÓN PERMITIDA
3
O1 – REPORTE CONSOLIDADO
NODO: A3*2
TÍTULO: ESTABLECER PARÁMETROS PARA USUARIOS Y DEPARTAMENTOS
Núm.: M3-P2-001
Página 13


20 de mayo de 2018
Flower Village Ecuador
C.1 - LEYES REGLAMENTOS
I.1 REPORTE CONSOLIDADO
ANALIZAR LA INFORMACIÓN
1
REPORTE DEL ANÁLISIS DE LA INFORMACIÓN
SEGREGACIÓN DE LA INFORMACIÓN
2
REPORTE CONSOLIDADO
DISEÑO DEL INFORME
3
O.1 INFORME DE MEJORAS
NODO: A3*3
TÍTULO:
INFORME PARA LA DIRECCIÓN ESTRATÉGICA
Núm.: M3-P3-003
Página 14

CAPÍTULO III

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para Flower Village Ecuador, la gestión y disponibilidad de la información es fundamental, razón por la cual se tiene un compromiso con la seguridad, con el fin de prevenir riesgos y generar conciencia en los usuarios. El área de TICS consciente de la mala gestión de la información, en su servicio de storage; propone el diseño de una política de seguridad de la información como una herramienta para identificar y mitigar riesgos.

El análisis de riesgos a los que está sujeto servicio de **storage** el mismo que es administrador por el área de TICS, es un requerimiento solicitado por la **BACS** para completar la certificación, sin embargo, no es único campo al cual se limitará ya que a futuro debe abarcar las distintas áreas de la empresa, el cumplimiento de esta política será liderada permanentemente por el **Oficial de Seguridad de la Información**. La política debe ser revisada continuamente tanto por el área de TICS, como por la gerencia.

3.1 Políticas generales de seguridad de la información

Antes de exponer los lineamientos generales se debe conformar un **Comité de Seguridad de la Información** (anexo 3)**,** integrado por: Gerente General o delegado (quien presidirá), Gerente de Riesgos o su delegado, Gerente de Talento Humano y Gerente de Tecnologías, sus funciones principales son:

- Verificar el cumplimiento de la política y alinearla dentro de las normas institucionales.
- Gestionar la mejora continua y colocarlo en vigencia a través de la máxima autoridad de la institución, así como el cumplimiento por parte de los funcionarios de la institución
- Vigilar la investigación de los incidentes relativos a la seguridad.
- Incentivar iniciativas para mejorar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Promover la capacitación del personal sobre la importancia de la seguridad de la información dentro de la institución.

- Designar custodios de la información en las diferentes áreas de la entidad, a través de un documento físico y electrónico.
- Gestionar recursos económicos, tecnológicos y humanos, para la gestión de la seguridad de la información.
- Designar formalmente a un funcionario como Oficial de Seguridad de la Información **(el mismo no pertenece al área de TICS y solo se reportará a la máxima autoridad de la institución)** quien actuará como coordinador del Comité de Seguridad de la Información.

Una vez conformado este comité se establece lo siguiente:

1. Los activos de información de Flower Village Ecuador, serán identificados y catalogados para definir estrategias de protección.
2. El área de TICS de Flower Village Ecuador definirá e implantará controles para proteger la información en el servicio de **storage** para evitar, accesos no autorizados, perdida de integridad y garantizar disponibilidad para los usuarios.
3. Todos los usuarios son responsables de proteger la información a la cual accedan y compartan, para evitar su pérdida, alteración, destrucción o uso indebido.
4. Se realizarán auditorías y controles periódicos sobre la Política de Seguridad de la Información.
5. Solo se permitirá el uso de software de backup que haya sido autorizado, administrado y adquirido legalmente por la empresa Flower Village Ecuador.
6. Es responsabilidad de todos los usuarios de la empresa Flower Village Ecuador reportar inconvenientes con la información que trabajan o que comparten con otros usuarios, el procedimiento para reportar un incidente es el siguiente:
   - Realizar una captura de pantalla de la información o archivos con problemas
   - Respaldar en usb, las capturas y entregar a su inmediato superior, enviar por correo a su superior y con copia a la siguiente dirección (sistemas@flowervillage.ec)
   - Está terminantemente prohibido dialogar de este problema con cualquier persona, que no sea el Oficial de Seguridad de la Información
7. Violar las Políticas de la Seguridad de la Información conlleva que el usuario/s serán reportados, sus acciones registradas y monitoreadas, con el fin de presentar un informe detallado si el caso lo amerita.

Acuerdos de confidencialidad

[ISO/IEC 27001:2005 A.6.1.5]

Todos los usuarios de **Flower Village Ecuador** deben aceptar los acuerdos de confidencialidad definidos por la Empresa, los cuales reflejan los compromisos de salvaguardar y usar la información de acuerdo con los criterios establecidos en ella. En el caso de terceros, se deberá firmar contratos los mismos deben incluir una cláusula de confidencialidad, los estatutos que contengan se deben estar orientados a salvaguardar la continuidad del negocio.

Riesgos relacionados con terceros

[ISO/IEC 27001:2005 A.6.2.2]

Flower Village Ecuador en su área de TICS debe identificar los posibles riesgos que pueden generar la administración, procesamiento o gestión de la información; por parte de terceros, para establecer los controles necesarios en su servicio de storage. Estos controles de deben establecer a partir de un análisis de riesgos, posteriormente deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

Uso adecuado de los activos

[ISO/IEC 27001:2005 A.7.1.3]

El acceso a documentos digitales propios o compartidos por cada usuario o departamento, serán determinados por **Comité de Seguridad de la Información y** la **Dirección Estratégica,** en el caso de terceros se necesitará un documento donde conste el grupo de usuarios y los privilegios. Todos los usuarios y terceros que manipulen información durante su permanencia en la empresa deben firmar un **"acuerdo de confidencialidad de la información"**, donde individualmente se comprometan a no divulgar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerada como un **"incidente de seguridad".**

Acceso a Internet

El uso adecuado de este recurso conlleva el monitorio, la verificación y el control; considerando los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, web proxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas por la empresa y supervisadas por el área de TICS.
- El intercambio no autorizado de información de propiedad de Flower Village Ecuador, de sus clientes; con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b) Flower Village Ecuador debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios y/o terceros (en este último caso se debe tomar en cuenta si se están conectando remotamente, así como cuando se encuentren dentro de cualesquiera de las fincas). Es fundamental evaluar las actividades realizadas durante la navegación, de acuerdo a las normas dispuestas por la Gerencia.
c) Cada uno de los usuarios es responsable del uso adecuado de este recurso y no está permitido realizar prácticas ilícitas o mal intencionadas que atenten contra usuarios de la misma empresa o terceros.
d) Los usuarios y/o terceros, no pueden asumir en nombre de Flower Village Ecuador, en encuestas de opinión, foros u otros medios similares.
e) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad, ni la protección de la información de Flower Village Ecuador.

Correo electrónico

Los usuarios y/o terceros autorizados a quienes Flower Village Ecuador a través de su área de TICS les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico solo debe ser usada para funciones asignadas y de conformidad a las normas establecidas por la Gerencia, no podrá ser utilizada a título personal, es decir para suscribir la cuenta a publicidad, material pornográfico, o que atente contra la empresa y su productividad.
b) Los correos y la información contenida en cada cuenta son propiedad del Flower Village Ecuador y cada usuario, como responsable de su cuenta, debe mantener solamente los mensajes relacionados con el desarrollo de sus actividades.
c) El tamaño de los buzones de correo es determinado por el área de TICS de acuerdo con las necesidades de cada usuario y previa autorización del Director de Sistemas.
d) El tamaño y recepción de mensajes, así como las características propias de cada uno de estos; deberán ser definidos e implementados por el área de TICS.
e) No es permitido:
    - Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico de la empresa, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
    - Utilizar la dirección de correo electrónico o dominio @flowervillage.ec como punto de contacto en comunidades interactivas tales como *Facebook* y/o *Twitter*, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
    - Enviar archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
    - El envío de archivos de música y videos.
f) Envió de información de la empresa a cuentas personales, exceptuando el área de ventas.
g) El envío masivo de mensajes publicitarios corporativos, en el caso de realizar dicha práctica se debe contar con la aprobación de la Gerencia y poner en conocimiento al área TICS. En el caso de terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución.

h) Toda información de Flower Village Ecuador generada con herramientas ofimáticas y que deba ser enviada a clientes debe ser protegida, utilizando las características de seguridad que brindan las mismas herramientas y ascesodaros por el área de TICS.

Recursos tecnológicos

Los recursos tecnológicos asignados por el área de TICS de la empresa Flower Village Ecuador a sus usuarios y/o terceros establecen que:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de Flower Village Ecuador es responsabilidad del área de TICS.

b) Los usuarios no deben realizar cambios en la configuración de los equipos de trabajo.

c) El área de TICS define cuando y como actualizar las aplicaciones instaladas en cada estación de trabajo.

d) Únicamente los usuarios y terceros autorizados por el área de TICS, previa solicitud escrita por parte del representante de área que lo requiera, pueden conectarse a la red inalámbrica de Flower Village Ecuador.

e) El uso de redes WIFI externas por usuarios con equipos portátiles fuera de la oficina y que requieran una conexión a la infraestructura de Flower Village Ecuador, deben utilizar una conexión estrictas normas de seguridad establecidas por el área de TICS.

f) En caso de realizar soporte remoto a dispositivos, equipos o servidores de la infraestructura de Flower Village Ecuador; el personal del área de TICS, deberá llevar una bitácora e informar al Director de Sistemas.

g) La sincronización de dispositivos móviles, como smartphones, GPS, Tablet u otros dispositivos electrónicos, deben estar autorizados de por el área de TICS.

Control de acceso físico

[ISO/IEC 27001:2005 A.9.1]

La infraestructura, los sistemas de información y comunicaciones, son áreas de acceso restringido, por lo cual deben contar con controles que permitan proteger, auditar y mantener la continuidad del negocio. En consecuencia, dichas áreas también deben cumplir requerimientos

ambientales (temperatura, humedad, etc.), especificados por los fabricantes de tal forma que al producirse un incidente se puede responder de una manera adecuada.

Segregación de funciones

[ISO/IEC 27001:2005 A.10.1.3]

Toda tarea o función en la cual los usuarios necesiten de acceso a la infraestructura tecnológica y a los sistemas de información, deben contar con niveles de acceso y privilegios, para reducir las incidencias dentro de la empresa.

En concordancia:

- El uso del storage de la empresa Flower Village Ecuador, debe constar con reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere o audite.
- Es necesario que el nivel más alto de usuario en el sistema pueda ser auditado.
- Las funciones de soporte y operadores, deben estar claramente segregadas.

Protección contra software malicioso

[ISO/IEC 27001:2005 A.10.4]

Flower Village Ecuador establece que los equipos informáticos (de propiedad de la empresa) deben estar protegidos mediante software de seguridad y aplicaciones de terceros que impidan en acceso a la red empresarial, es responsabilidad del área de TICS analizar y autorizar el uso de estas herramientas, así como su administración, manteamiento, y documentación en caso de una auditoria.

Así mismo, el área de TICS de la empresa Flower Village Ecuador define los siguientes parámetros:

a) No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por el área de TICS.

- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código, bath, script; diseñado para auto dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

Copias de respaldo

[ISO/IEC 27001:2005 A.10.5]

El área de TICS de la empresa Flower Village Ecuador después de identificar la información crítica por usuario y departamento, la misma que se almacena en el storage, debe proceder a resguardar la misma con el uso de mecanismos y controles entre los cuales se plantea:

- A nivel Físico:
    - Implementando controles de acceso
    - Alarma de incendios
    - Video seguridad
- A nivel de Red:
    - Segmentando la red (con el uso de vpn y vlan)
    - Monitoreando el acceso en los swith y enlaces wifi
- A nivel lógico:
    - Revisando parches de seguridad en todos los equipos de la red
    - Doble factor de autenticación
    - Backups programados

En cuanto a los backups se plantea seguir el siguiente proceso:

N°	Actividad (diagrama de flujo)	Descripción de la actividad	Responsable	Documento Registro
1	Inicio	Inicio del procedimiento		
2	Determinar proceso de backup	Se identifica los archivos a respaldar tanto en los servidores, como en los equipos de las diferentes áreas	Ing. Sistemas o Soporte	
3	Identificar archivos y/o base de datos	Se identifica el número de archivos y/o bases de datos para el respaldo	Ing. Sistemas o Soporte	
4	Determinar mecanismos	Se determinan los mecanismos de copias de respaldo según la base de datos y equipos	Ing. Sistemas o Soporte	Bitácora de backup
5	Verificar archivos	Se verifican los archivos log del aplicativo utilizado para la copia de seguridad	Ing. Sistemas o Soporte	
6	Verificar copias de restauración	Se verifica las copias para la restauración, 2 veces al mes en entornos de prueba	Ing. Sistemas o Soporte	Bitácora de verificación
7	Realizar copia por segunda vez	Si el archivo log del servidor indica un error, se realiza copia por segunda vez	Ing. Sistemas o Soporte	
8	Respaldo de copias	Se graba de manera diaria, una copia en un dispositivo externo, así como una tarea de sincronización en cloud la misma debe una alerta a una dirección de correo electrónico	Ing. Sistemas o Soporte	Bitácora de de copias
	Fin	Fin del procedimiento		

Figura 27. Procesos para realizar un backup

Elaborado por: Autor de la investigación

Intercambio de información

[ISO/IEC 27001:2005 A.10.8]

Flower Village Ecuador firmará acuerdos de confidencialidad con los usuarios, clientes y terceros (anexo 3) que por diferentes distintas razones solicitan información restringida o confidencial de la empresa, las responsabilidades para proveer esta información deben estar estipuladas en los acuerdos que firmen cada una de las partes.

Los usuarios o departamentos custodios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma, toda esta información debe entregarse al área de TICS para implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

Control de acceso lógico

[ISO/IEC 27001:2005 A.11.1]

El control de acceso para el servicio de storage de Flower Village Ecuador es asignado de acuerdo a los requerimientos de seguridad, así como normas establecidas por **Comité de Seguridad de la Información y** la **Dirección Estratégica**.

El área de TICS como responsable la infraestructura tecnológica de Flower Village Ecuador creara los perfiles para los usuarios los cuales deben ser revisados periódicamente y documentados para una posterior auditoria.

La autorización para el acceso al servicio de storage debe ser otorgada no solo por el área de TICS, sino también solicitada por jefe de cada área, como punto final todos los involucrados deben firmar una constancia la misma que se registrara en la bitácora del área de TICS.

Cualquier usuario interno o externo que requiera acceso remoto al servicio de storage, debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

Gestión de contraseñas de usuario

[ISO/IEC 27001:2005 A.11.2.3]

Los recursos de información identificados como críticos deben tener asignados niveles de acceso con base en los perfiles que cada usuario requiera para el desarrollo de sus funciones, los mismos serán definidos y aprobados por las áreas de negocio y administrados por el área de TICS.

Todo usuario o tercero que requiera usar el servicio de storage debe estar debidamente autorizado y acceder mediante su usuario (ID) y contraseña (password) asignado por el área de TICS, finalmente cada usuario debe ser responsable por sus credenciales de acceso.

Escritorio y pantalla limpia

[ISO/IEC 27001:2005 A.11.2.4]

El área de TICS proveerá un mismo papel tapiz y el protector de pantalla para cada equipo de trabajo, el mismo se activará automáticamente después de (5) minutos de inactividad y solo se podrá desbloquear con la contraseña del usuario.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- El análisis, diseño o implementación de una Norma ISO, debe tener dos aspectos fundamentales, debe ser clara tanto con las personas involucradas y tener el apoyo de las autoridades.
- Es necesario concientizar y capacitar al personal continuamente, sobre la importancia de la seguridad de la información.
- Aunque la norma provea parámetros y sugerencias, es fundamental estudiar casos reales; sobre el uso de la norma.
- En el caso particular de la empresa Flower Village Ecuador, el manejo de la información en el servicio de storage; tiene muchas falencias como se explicó en esta investigación, se están llevando a cabo los correctivos, pero solo es el primer paso, para obtener una certificación.

4.2 Recomendaciones

- Es fundamental realizar un correcto análisis de las necesidades de la empresa, para identificar los riesgos, estos deben estar documentados, antes de realizar el diseño de la política de seguridad de la información.
- Toda esta investigación está orientada, en lo posible a ser clara y puntual, buscando ser a fin con las actividades diarias del personal, los objetivos de la empresa y las buenas prácticas propuestas por los estándares tomados como referencia.
- Aunque el objetivo es que la norma entre en funcionamiento, la empresa debe realizar campañas de concientización sobre su importancia.

BIBLIOGRAFÍA

Academy. (2017). *Precios y opciones de los paquetes de documentación sobre ISO 27001 e ISO 22301.* Obtenido de http://bit.ly/2hTzZ4Z

Alianza Empresarial para el Comercio Seguro Basc. (2017). *La Norma BASC*. Obtenido de World Basc Organization: http://bit.ly/2iPQ0K7

Alvarado Peñaranda, M. (29 de Mayo de 2015). *Áreas principales de la norma ISO 27002.* Obtenido de http://bit.ly/2n21JcO

Andrés, A., & Gómez, L. (2009). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* Madrid, España: Aenor. Obtenido de http://bit.ly/2k0b3ga

Arias, F. G. (2012). *El Proyecto de Inestigación.* Caracas, Venezuela: PISTEME.

Arora, V. (2010). *Comparing different information security standards: COBIT v s. ISO 27001 (Comparación de diferentes estándares de seguridad de la información: COBIT v s. ISO 27001).* New York: Pearson. Obtenido de http://bit.ly/2iQQuPQ

Arribas, M. (2004). Diseño y validación de cuestionarios. *Matronas Profesión, 5*(17), 5-7. Obtenido de http://bit.ly/1P3D36U

Avilés Armijos, J. M., & Uyaguari Guartatanga, M. E. (2012). *Diseño de una política de seguridad para la empresa de Telecomunicaciones PUNTONET en la ciudad de Cuenca, en base a las normas de seguridad ISO 27001 y 27011 como líneas base para las buenas prácticas de tratamiento y seguridad de la información.* Cuenca: se. Obtenido de Universidad Politécnica Salesiana Ecuador Repositorio Digital: https://dspace.ups.edu.ec/bitstream/123456789/2158/14/UPS-CT002406.pdf

Ayres Sfreddo, J., & Flores, D. (2012). Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais. *Perspectivas em Ciência da Informação, 17*(2), 158-178. Obtenido de http://bit.ly/2zUJcnz

Baquero, K. (26 de Octubre de 2012). *COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas).* Obtenido de http://bit.ly/2ySHiDF

Benjumea, O. (2 de Mayo de 2016). *¿Sabes diferenciar la ISO 27001 y la ISO 27002?* Obtenido de redseguridad.com: http://bit.ly/2jIF40n

BITCompany. (9 de Abril de 2015). *CobiT: Un marco de referencia para la información y la tecnología.* Obtenido de http://bit.ly/2n0qohY

Burgos Salazar, J., & Campo, P. G. (2009). Modelo Para Seguridad de la Información en TIC. En J. Bustos Gómez (Ed.), *Encuentro de Informática y Gestión 2009. 488*, págs. 241-242. Concepción: CEUR-WS. Obtenido de http://ceur-ws.org/Vol-558/

CONECTA.ec. (2016). *Porqué mi organización debe certificarse en ISO 27001.* Quito. Obtenido de CONECTA.ec Tried and Trusted: http://bit.ly/2hblvNP

Corporación Nacional de Telecomunicaciones CNT. (29 de Mayo de 2015). *CNT única empresa pública en el Ecuador que obitne certificación ISO 27001.* Quito: Norma. Obtenido de http://bit.ly/2xnIECx

Definiciones-de.com. (17 de Junio de 2010). *Definición de desagregar - ALEGSA © .* Obtenido de http://www.definiciones-de.com/Definicion/de/desagregar.php

Disterer, G. (16 de Abril de 2013). ISO/IEC 27000, 27001 and 27002 for Information (ISO/IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información). *Journal of Information Security, 4*, 92-100. Obtenido de http://bit.ly/2A7a3gC

EcuRed. (2011). *ISO/IEC 27002.* Obtenido de EcuRed Conocimiento con todos y para todos: http://bit.ly/2BaUdyy

El portal de ISO 27002 en Español. (2012 - 2016). *Políticas de seguridad.* Obtenido de http://bit.ly/2jZYGAW

ENCONTEXTO. (23 de Enero de 2010). *Metodología de la Investigación.* Obtenido de ENCONTEXTO Información todos los días: http://bit.ly/2zE3frH

Farias-Elinos, M., Mendoza-Diaz, M. C., & Gómez-Velazco, L. (2003). Techno-Legal aspects of Information Society and New Economy: an Overview. *Information Society, 4*(23), 27-35.

Franco, D. C., & Guerrero, C. D. (13 de Agosto de 2016). Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002. *Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2016)* (págs. 2-3). Cancun: Ariel. Obtenido de http://bit.ly/2zEW960

Galán Amador, M. (13 de Septiembre de 2011). *La investigación documental, qué es y en qué consiste.* Obtenido de El pensante: http://bit.ly/2i3IyOh

García, J. (2017). *ITIL vs COBIT, características de COBIT.* Barcelona. Obtenido de netmind: http://bit.ly/2jo2LLn

Graterol, R. (Marzo de 2011). *Metodos de Investigación.* Sevilla: Pax. Obtenido de http://bit.ly/2fGwoGL

Guana, C. (11 de Junio de 2008). *Más información sobre ISO 27005:2008.* Buenos Aires: Piramide. Obtenido de http://bit.ly/2jotZ4t

Hernández Sampieri, R. F. (2003). *Metodología de la investigación.* México: McGraw-Hill.

Ionescu, C. (2016). Challenges Generated by the implementación of the it standards Cobit 4.1, ITIL V3 and ISO/IEC 27002 in enterprises. *The Bucharest Academy of Economic Studies*, 3-15. Obtenido de The Bucharest Academy of Economic Studies: http://www.ecocyb.ase.ro/articles%203.2009/Pavel%20Nastase.pdf

iStock, A. (2016). *Definición de Investigación de Campo.* Obtenido de http://bit.ly/2A56IOZ

Kosutic, D. (2017). *Diferencias y similitudes entre ISO 27001 e ISO 27002.* Recuperado el 3 de Diciembre de 2017, de 27001academy: http://bit.ly/2AQKhhz

Ladino, M. I., & Villa, P. A. (Abril de 2014). Fundamentos de ISO 27002 y su aplicacion en las empresas. *Scientia et Technica, 47*, 334. Obtenido de http://bit.ly/2jocjpE

Marín, A. (26 de Noviembre de 2014). *Técnicas de Levantamiento de Requerimientos.* Obtenido de http://bit.ly/2n0s7nm

Mayta, Y. (21 de Marzo de 2013). *Método inductivo - deductivo.* Obtenido de SlideShare: http://bit.ly/2i8n9Dw

Medeiros, C. R. (2001). *La seguridad de la información: aplicación de las medidas y herramientas para la seguridad de la información.* Santa Catarina: Universidad de la región de Joinville. Obtenido de http://bit.ly/2Bogqua

Menéndez, A. (Noviembre de 2015). Confiabilidad. *CES* , 1-4. Obtenido de http://bit.ly/2k0A5Mg

Montaño Orrego, V. (Junio de 2011). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano, 18*(46), 21-34. Obtenido de http://bit.ly/2hQHA49

Montoya, J. (10 de Febrero de 2009). Estándar Internacional ISO/IEC 27002. *Estándares Internacionales*, 15-39. Obtenido de http://bit.ly/2zoe78Q

NEXTECH. (2010). Qué es el ciclo de vida de ITIL. En D. Soto, *Etapas del Ciclo de Vida* (pág. 23). Lima: Norma. Obtenido de NEXTECH Education Center: http://bit.ly/2A7pkym

Peltier, T. R. (2005). *Information Security Risk Analysis.* Chicago: CRC Press.

Pérez Porto, J., & Merino, M. (2012). *Método Inductivo.* Obtenido de Definicion.de: http://bit.ly/2hnuYVF

Pressman, R. (2006). *Ingenieria del Software.* Cali: Norma. Obtenido de http://bit.ly/2AxdZYL

Romo Villafuerte, D., & Valarezo Constante, J. (2012). *Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil.* Guayaquil, Guayas, Ecuador: se. Recuperado el 3 de Diciembre de 2017, de http://bit.ly/2nu3HTR

Secretaría Nacional de Gestión de la Política. (15 de Junio de 2016). *Esquema Gubernamental de Seguridad de la Información (EGSI).* Obtenido de http://bit.ly/2n4pAso

Selltiz, C., Jahoda, M., & otros. (1970). *Métodos de investigación en las relaciones sociales* . Madrid: RIALP.

Servicio Ecuatoriano de Normalización. (05 de ABRIL de 2016). *Tecnologías de la información técnicas de seguirdad codigo de prácticas para los controles de seguridad de la información.* Obtenido de http://bit.ly/2BnGk0M

Servicio Ecuatoriano de Normalización. (05 de Abril de 2016). Tecnologías de la inforamción técnicas de seguridad codigo de prácticas para los controles de seguridad de la inforamción. En *NTE INEN-ISO/IEC 27002* (págs. 28-34). Quito: se. Obtenido de http://bit.ly/2BnGk0M

SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información. (21 de Mayo de 2015). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Obtenido de http://bit.ly/2hT9OeK

SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información. (28 de Septiembre de 2017). *¿Cuál es la situación de la norma ISO 27001 en Sudamérica?* Obtenido de http://bit.ly/2A60AWM

Silva Netto, A., & Pinheiro da Silveira, M. A. (Diciembre de 2016). Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. *JISTEM - Journal of Information Systems and Technology Management, 4*(3), 375-397. Obtenido de Scielo: http://bit.ly/2Ablsd3

Sistemas de Gestión de Seguridad de la Información SGSI. (14 de Junio de 2016). *La norma ISO 27002 complemento para la ISO 27001.* Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Informacióncerrojo: http://bit.ly/2osTMce

Tamayo, M. T. (2004). *El Proceso de la Investigación Cientifica.* Mexico: LIMUSA Grupo Noriega Editores.

Universidad de la Plata. (2016). *IRAM-ISO/IEC 17799 Código de práctica para la gestión de la seguridad de la información Serie ISO 27000.* La Plata: se.

Universidad Pedagógica Experimental Libertador. (18 de Junio de 2013). *Tipo y Modalidad de la Investigación. Ejemplo.* Obtenido de http://bit.ly/2k3k2xu

Valencia-Duque, F. J., & 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. *Revista Ibérica de Sistemas e Tecnologias de Informação*(22), 73-88. Obtenido de http://bit.ly/2k0rf14

Vásquez Hidalgo, I. (18 de Diciembre de 2005). *Tipos de estudio y métodos de investigación.* Obtenido de Gestiopolis: http://bit.ly/2A7NubC

Velásquez, I. (2015). *Modelamiento de los procesos de auditoría en seguridad de la información asociados a los dominios 6, 8, 13 Y 14 del anexo A de La norma Iso 27001 mediante una herramienta de flujo de trabajo.* Pereira: se. Obtenido de Universidad Tecnológica de Pereica: http://bit.ly/2Abd4dI

Villegas Arciniegas, M. G. (2017). *Examen de Auditoría Integral al área de Recursos Humanos de la Empresa Flower Village Cia. Ltda. por el período 2013.* Quito: se. Obtenido de http://bit.ly/2k0V2a0

Voutssas M., J. (6 de Abril de 2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica, 24*(50), 127-155. Recuperado el 3 de Diciembre de 2017, de Scielo: http://bit.ly/2AE37YV

ANEXOS

Anexo 1. Cuestionario para evaluación del Área de TICS

Cuestionario para evaluación del Área de TICS

Nombre: Fecha:

Cargo:

Tiempo de trabajo en la empresa:

Instrucciones:

- Responda las preguntas lo más detallado posible,
- Puede elegir varias respuestas en las pregunta de selección múltiple

1. Una amenaza se puede definir como:

   a) Una medida orientada a mitigar de alguna forma los riesgos que puedan existir en una empresa.
   b) Una vulnerabilidad identificada dentro de una empresa.
   c) Un agente o evento que puede explotar una vulnerabilidad identificada dentro de una empresa.
   d) Una serie de eventos desafortunados que activan un plan de emergencia en una empresa

2. Explique brevemente como se ha enfrentado una amenaza según su cargo en el área de TICS

3. Según su experticia que considera como controles de seguridad, enliste al menos 3

4. Cuál de los siguientes puede considerarse como un control poco confiable para el manejo de la información

   a) Los controles de preventivos combinados con los controles manuales.
   b) Los controles preventivos combinados con los controles automáticos.
   c) Los controles detectives combinados con los controles manuales.
   d) Los controles detectives combinados con los controles automatizados.

5. Explique cual es el procedimiento para el manejo de la información, en el servicio de storage

Anexo 2. Acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD

El objeto de garantizar la confidencialidad la información [**entre las partes implicadas**], se hace necesario la firma de un acuerdo que garantice unos niveles de confianza entre las partes. El documento se firmará una vez aceptado y firmado el (**tipo: acuerdo,...**] por ambas partes.

DE UNA PARTE: **[nombre de la organización]**y en su nombre y representación (con poder suficiente para ello) D/Dña. **[nombre completo],** en calidad de **[cargo, administrador, apoderado,...]**

DE OTRA PARTE: **[nombre de la organización].** y en su nombre y representación **(con poder suficiente para ello)** D/Dña. [nombre completo], en calidad de **[cargo, administrador, apoderado,...]**

Reunidos en **[lugar de la firma del contrato]**, a **[día]** de **[Mes]** de **[Año]**

EXPONEN

I – Que las partes, anteriormente citadas, están interesadas en el desarrollo del presente contrato, para lo cual, aceptaron celebrar el presente Acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirá la custodia y no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, Propietario y «Destinatario» de la referida información.

II – Que las partes, en virtud de lo anteriormente expuesto, convinieron que el presente Acuerdo de Confidencialidad se rija por la normativa aplicable al efecto y, en especial por las siguientes.

CLÁUSULAS

PRIMERA - Definiciones

A los efectos del presente Acuerdo, los siguientes términos serán interpretados de acuerdo con las definiciones anexas a los mismos. Entendiéndose por:

- «Información propia»: tendrá tal consideración y a título meramente enunciativo y no limitativo, lo siguiente: descubrimientos, conceptos, ideas, conocimientos, técnicas, diseños, dibujos, borradores, diagramas, textos, modelos, muestras, bases de datos de cualquier tipo, aplicaciones, programas, marcas, logotipos, así como cualquier información de tipo técnico, industrial, financiero, publicitario, de carácter personal o comercial de cualquiera de las partes, esté o no incluida en la solicitud de oferta
presentada, independientemente de su formato de presentación o distribución, y aceptada por los «Destinatarios».

- «Fuente»: tendrá la consideración de tal, cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sea ella la que suministre la Información Propia y/o cualquiera de los implicados (accionistas, directores, empleados, ...) de la empresa o la organización.

- «Destinatarios»: tendrán la consideración de tales cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sea ellos quienes reciban la Información Propia de la otra parte.

SEGUNDA.- Información Propia.

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, técnicos, y/o industriales suministrada a la otra parte como consecuencia de la solicitud de Oferta para el desarrollo del presente proyecto objeto del contrato, o en su caso, de los acuerdos a los que se lleguen (con independencia de que tal transmisión sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea) tendrá consideración de información confidencial y será tratada de acuerdo con lo establecido en el presente documento. Esa información, y sus copias y/o

reproducciones tendrán la consideración de «Información propia» los efectos del presente acuerdo.

TERCERA.- Exclusión del Presente Acuerdo.

No se entenderá por «Información propia», ni recibirá tal tratamiento aquella información que:
I – Sea de conocimiento público en el momento de su notificación al «Destinatario» o después de producida la notificación alcance tal condición de pública, sin que para ello el «Destinatario» violentara lo establecido en el presente acuerdo, es decir, no fuera el «Destinatario» la causa o «Fuente» última de la divulgación de dicha información.
II – Pueda ser probado por el «Destinatario», de acuerdo con sus archivos, debidamente comprobados por la «Fuente», que estaba en posesión de la misma por medios legítimos sin que estuviese vigente en ese momento algún y anterior acuerdo de confidencialidad al suministro de dicha información por su legítimo creador.
III – Fuese divulgada masivamente sin limitación alguna por su legítimo creador.
IV – Fuese creada completa e independientemente por el «Destinatario», pudiendo este demostrar este extremo, de acuerdo con sus archivos, debidamente comprobados por la «Fuente».

CUARTA.- Custodia y no divulgación.

Las partes consideran confidencial la «Información propia» de la otra parte que le pudiera suministrar y acuerdan su guarda y custodia estricta, así como a su no divulgación o suministro, ni en todo ni en parte, a cualquier tercero sin el previo, expreso y escrito consentimiento de «Fuente». Tal consentimiento no será necesario cuando la obligación de suministrar o divulgar la «Información propia» de la «Fuente» por parte del «Destinatario» venga impuesta por Ley en vigor o Sentencia Judicial Firme.

Este Acuerdo no autoriza a ninguna de las partes a solicitar o exigir de la otra parte el suministro de información, y cualquier obtención de información de/o sobre la «Fuente» por parte del «Destinatario» será recibida por éste con el previo consentimiento de la misma.

QUINTA.- Soporte de la «Información propia».

Toda o parte de la «Información propia», papeles, libros, cuentas, grabaciones, listas de clientes y/o socios, programas de ordenador, procedimientos, documentos de todo tipo o tecnología en el que el suministro fuese hecho bajo la condición de «Información propia», con independencia del soporte que la contuviera, tendrá la clasificación de secreta, confidencial o restringida

SEXTA.- Responsabilidad en la Custodia de la «Información propia».

La «Información propia» podrá ser dada a conocer por el «Destinatario» o sus directivos y/o sus empleados, sin perjuicio de que el «Destinatario» tome cuentas medidas sean necesarias para el exacto y fiel cumplimento del presente Acuerdo, debiendo necesariamente informar a unos y otros del carácter secreto, confidencial, o restringido de la información que da a conocer, así como da existencia del presente Acuerdo.

Así mismo, el «Destinatario» deberá dar a sus directivos y/o sus empleados, las directrices e instrucciones que considere oportunas y convenientes a los efectos de mantener el secreto, confidencial, o restringido de la información propia de la «Fuente». El «Destinatario» deberá advertir a todos sus directivos, empleados, etc., que de acuerdo con lo dispuesto en este acuerdo tengan acceso a la «Información propia», de las consecuencias y responsabilidades en las que el «Destinatario» puede incurrir por la infracción por parte de dichas personas, de lo dispuesto en este Acuerdo.

Sin perjuicio de lo anterior, la «Fuente» podrá pedir y recabar del «Destinatario», como condición previa al suministro de la «Información propia», una lista de los directivos y empleados que tendrán acceso a dicha información, lista que podrá ser restringida o reducida por la «Fuente».

Esta lista será firmada por cada uno de los directivos y empleados que figuren en ella, manifestando expresamente que conocen la existencia del presente Acuerdo y que actuarán

de conformidad con lo previsto en él. Cualquier modificación de la lista de directivos y/o empleados a la que se hizo referencia anteriormente será comunicada de forma inmediata a la «Fuente», por escrito conteniendo los extremos indicados con anterioridad en este párrafo.

Sin perjuicio de lo previsto en los párrafos anteriores, cada parte será responsable tanto de la conducta dos sus directivos y/o empleados como de las consecuencias que de ella se pudieran derivarse de conformidad con lo previsto en el presente Acuerdo.

SÉPTIMA.- Responsabilidad en la custodia de la «Información propia».

El «Destinatario» será responsable de la custodia de la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», en orden a su tratamiento, como secreta, confidencial o restringida, en el momento presente y futuro, salvo indicación explicita de la «Fuente».
Al objeto de garantizar esta custodia, se deberá devolver la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», a la terminación de las relaciones comerciales, o antes, si fuera requerido por la «Fuente» y respondiendo a los daños y perjuicios correspondientes, en el caso de incumplimiento de lo aquí dispuesto. (En aquellos casos en los que no fuera necesaria la devolución de la «Información propia» deberá eliminarse este párrafo)

OCTAVA.- Incumplimiento.

El incumplimiento de las obligaciones de confidencialidad plasmadas en este documento, por cualquiera de las partes, sus empleados o directivos, facultará a la otra a reclamar por la vía legal que estime más procedente, a la indemnización de los daños y perjuicios ocasionados, incluido el lucro cesante.

NOVENA.- Duración del Acuerdo de Confidencialidad.

Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, aún después de terminar sus relaciones comerciales.

DECIMA.- Legislación Aplicable

El presente Acuerdo de Confidencialidad se regirá por la Legislación Española, y cualquier disputa, controversia o conflicto en cuanto a la interpretación o ejecución del presente Acuerdo será sometido a la jurisdicción de los Tribunales de (Valladolid), con exclusión de cualquier otro que pudiera corresponder a las partes, al que en este momento renuncian.

Y en prueba de esta conformidad, las partes firman o presente acuerdo, por duplicado y a un solo efecto, en el lugar y fecha ut supra.

Entidad	Entidad
_____	_____
Firma representante _____	Firma representante_____
CI. representante_____	CI. representante_____

Anexo 3. Acta de constitución del comité de seguridad de la información

ACTA DE CONSTITUCIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

En ..... con fecha.....reunidas las personas que a continuación se referencian:

....
en calidad de:..... en calidad de:.....

....
en calidad de:..... en calidad de:.....

....
en calidad de:..... en calidad de:.....

en cumplimiento de con los estatutos de la empresa Flower Village Ltda. para la de Seguridad e la Información se acuerda dar por constituido el Comité de Seguridad Información como organismo que velara por la integridad, disponibilidad, mitigación de riesgos; tanto el uso interno y externo de la información.

Dicho Comité estará integrado por las personas que se relacionan:

Por parte de la empresa:	Por parte de los representantes de los trabajadores:
Nombre:…… C.I.:…….	Nombre:…… C.I.…….
Firma:……	Firma:……
Nombre:…… C.I.:……	Nombre:…… C.I.:……
Firma:……	Firma……
Nombre:…… C.I.:……	Nombre:…… C.I.……
Firma:……	Firma……

En prueba de conformidad, los arriba firmantes certifican el presente documento en ……a……de……de 20……