SEGURIDAD DE LA INFORMACIÓN

Política para la seguridad de la información.
Asociación Colombiana de Exportadores de Flores
ASOCOLFLORES

TERMINOS Y CONDICIONES DE USO

Versión actual del documento: 1.0

ASOCOLFLORES G.M. Secretario General

TABLA DE CONTENIDO

1. INTRODUCCION

La Asociación Colombiana de Exportadores de Flores – ASOCOLFLORES- identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Asociación, razón por la cual es necesario que la Asociación establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por ASOCOLFLORES. Para la elaboración del mismo, se toman como base el capítulo décimo segundo del título primero de la Circular Básica Jurídica de la Superintendencia Financiera de Colombia, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013 y demás regulaciones aplicables.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de ASOCOLFLORES y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para ASOCOLFLORES y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información de ASOCOLFLORES, con el fin de regular la gestión de la seguridad de la información al interior de la Asociación.

3. ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- ✓ **Confidencialidad:** los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- ✓ **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- ✓ **Disponibilidad:** A los activos de información sólo pueden acceder por corto plazo los usuarios que tengan los permisos adecuados.

Para ello es necesario considerar aspectos tales como:

- ✓ **Autenticidad:** Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- ✓ **Posibilidad de Auditoría:** Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

ASOCOLFLORES G.M. Secretario General

- ✓ **Protección a la duplicación:** Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- ✓ **No repudio:** Los autores, propietarios y custodios de los activos de información se puede identificar plenamente
- ✓ **Legalidad:** Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.
- ✓ **Confiabilidad de la Información:** Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

4. DEFINICIONES Y GLOSARIO.

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la asociación y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Es un documento en los que los empleados de ASOCOLFLORES o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Asociación, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Centros de cableado: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Custodio del activo de información: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Guías de clasificación de la información: Directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Hacking ético: Es el conjunto de actividades para ingresar a las redes de datos y voz de la Asociación con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencia, el número de veces ocurrido o el origen (interno o externo).

Integridad: Es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: Es una lista ordenada y documentada de los activos de información pertenecientes a la Asociación.

Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: Es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de ASOCOLFLORES.

Responsable por el activo de información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por ASOCOLFLORES o de origen externo ya sea adquirido por la Asociación como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

5. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

La Asociación Colombiana de Exportadores de Flores -ASOCOLFLORES- garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- ✓ Secretario General, o un delegado especializado.
- ✓ Asistente de Secretario General, o un delegado especializado.
- ✓ Coordinador de Tecnología, o un delegado especializado.

En todo caso, dicha comisión o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a las directivas de la Asociación para su aprobación mediante resolución o acto jurídico correspondiente.

Los directores de dependencia, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsable de Seguridad de la Información y por tanto deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados por las directivas.

6. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

6.1. GENERALIDADES

La información es un recurso que tiene valor para la Asociación y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

La institución establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

6.2. ALCANCE

Esta política es de aplicación en el conjunto de dependencias que componen la Asociación, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la universidad a través de contratos o acuerdos con terceros y a todo el personal de ASOCOLFLORES, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

ASOCOLFLORES G.M. Secretario General

6.3. OBJETIVOS

a) Proteger, preservar y administrar objetivamente la información de ASOCOLFLORES junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.
b) Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la Asociación para asegurar su permanencia y nivel de eficacia.
c) Definir las directrices de ASOCOLFLORES para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

6.4. RESPONSABILIDAD

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Asociación Colombiana de Exportadores de Flores –ASOCOLFLORES-, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe. Las directivas institucionales aprueban esta política y son responsables de la autorización de sus modificaciones.

El Comité de Seguridad de la Información de la institución es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la Asociación. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Asociación.

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El coordinador de tecnología será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la Asociación, de promover el cumplimiento de la política con las respectivas dependencias y de aspectos inherentes a los temas tratados en la presente Política.

Los propietarios de activos de información (ver su definición en el glosario) son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

La Gerencia administrativa y Financiera cumplirá la función de notificar a todo el personal que se vincula contractualmente con la Asociación, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías relacionados a la misma. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Seguridad de la Información.

La Coordinación de Tecnología debe seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la entidad. Corresponde a la mencionada Coordinación determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Jefe de Almacén y el Jefe de Recursos Físicos.

El Secretario General verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la Asociación en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

7. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida).

Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo a la Coordinación de Tecnología brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

8. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

Todo el personal de la Asociación Colombiana de Exportadores de Flores -ASOCOLFLORES-, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La Coordinación de Tecnología debe mantener un directorio completo y actualizado de tales perfiles.

El Comité de Seguridad de la Información determina cuales son los atributos que deben definirse para los diferentes perfiles. Además, debe elaborar, mantener, actualizar, mejorar y difundir la política de Seguridad de la Información en la Asociación Colombiana de Exportadores de Flores -ASOCOLFLORES-.

ASOCOLFLORES G.M. Secretario General

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en la Coordinación de Tecnología y una copia de dicha información debe permanecer en archivo de la dependencia respectiva del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

9. SEGURIDAD FISICA Y DEL ENTORNO

9.1. ACCESO

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. La Coordinación de Tecnología elaborará y mantendrán las normas, controles y registros de acceso a dichas áreas.

9.2. SEGURIDAD DE LOS EQUIPOS

Los servidores que contengan información y servicios institucionales deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- ✓ Seguridad física.
- ✓ Detección de incendio y sistemas de extinción de conflagraciones.
- ✓ Controles de humedad y temperatura.
- ✓ Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la Coordinación de Tecnología. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito de la Coordinación de Tecnología.

Equipos claves de comunicaciones deben se alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

La Coordinación de Tecnología debe asegurar que la infraestructura de servicios de tecnología este cubierta por mantenimiento y soporte adecuados de hardware y software

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la Asociación el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta garantizando ambiente seguro y protegido como se mencionó anteriormente.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad. Las personas que extraigan información de cualquier equipo de computo, sea por medio de la utilización de una USB

o por medio del envió a discos virtuales como Dropbox o Google Drive sin la autorización de Asocolflores, será responsable laboral y/o penalmente, analizándose cada caso particular por parte de la Asociación.

10. ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES

10.1. REPORTE DE INVESTIGACION DE INCIDENTES DE SEGURIDAD

El personal de ASOCOLFLORES debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su director de dependencia a la Coordinación de Tecnología, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

En conformidad con la ley, ASOCOLFLORES podrá interceptar o realizar seguimiento a los incidentes que atenten contra la seguridad, por diferentes mecanismos previa autorización del Comité de Información, y en todo caso notificando previamente a los afectados por esta decisión.

10.2. PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos, técnicos y administrativos.

En todo caso y como control mínimo, las estaciones de trabajo de la Asociación deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de la estaciones no están autorizados a deshabilitar este control.

La coordinación de tecnología podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

La Coordinación de tecnología debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

10.3. COPIAS DE SEGURIDAD

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos establecidos. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de ASOCOLFLORES deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas. La información más sensible de cada dependencia debe permanecer

ASOCOLFLORES G.M. Secretario General

dentro del directorio compartido P: a ese directorio se le realizar una copia de seguridad de frecuencia semanal para su respaldo y será almacenada con frecuencia de máximo un mes por cada copia de seguridad.
La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. En este caso, los usuarios deben entregar al coordinador de tecnología las copias de seguridad, para su registro y custodia.

10.4. ADMINISTRACION DE CONFIGURACIONES DE RED

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Coordinación de Tecnología.

Todo equipo de tecnología debe ser revisado, registrado y aprobado por la Coordinación de Tecnología antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

10.5. INTERCAMBIO DE INFORMACIÓN CON ORGANIZACIONES EXTERNAS

Las peticiones de información por parte de entes externos o entes de control deben ser aprobadas por la Presidencia o por el Secretario General, y dirigida por dichos entes a los responsables de su custodia.

Toda la información institucional debe ser manejada de acuerdo a la legislación. (Sección 12 de esta Política)

10.6. INTERNET Y CORREO ELECTRONICO

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

10.7. INSTALACIÓN DE SOFTWARE

Todas las instalaciones de software que se realicen sobre sistemas de la Asociación deben ser aprobadas por la coordinación de tecnología.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. La coordinación de Tecnología debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde a la coordinación de Tecnología mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

11. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE SOFTWARE

Para apoyar los procesos operativos y estratégicos de la Asociación se debe hacer uso intensivo de las tecnologías de la Información y las comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio. La coordinación de tecnología debe elegir, elaborar, mantener y difundir los lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. La Asociación no debe emprender procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

12. CUMPLIMIENTO

Todo uso y seguimiento de los recursos de tecnología en la Asociación Colombiana de Exportadores de Flores – ASOCOLFLORES - debe estar de acuerdo a las normas y estatutos internos, así como a la legislación nacional en la materia, incluido pero no restringido a:

Constitución Política de Colombia
Ley 527/1999 "Ley de comercio electrónico"
NTC 27001:2006. "Sistema de Gestión de Seguridad de la Información"
ISO/IEC 17799:2005 "Information technology Security techniques Code of practice for information security management"
MECI 1000:2005 "Lineamientos generales para la implementación del Modelo Estándar de Control Interno para el Estado Colombiano".
NTCGP1000:2004 "Norma Técnica Colombiana de la Gestión Publica"
POLÍTICA DE USO DE INTERNET -ASOCOLFLORES- TRABAJADORES
POLÍTICA DE USO DE INTERNET -ASOCOLFLORES- CONTRATISTAS

13. REFERENCIAS

[1] ISO 27001:2005. Sistemas de gestión de Seguridad en la Información– Requerimientos.
[2] ISO/IEC 133351: 2004. Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones.
[3] ISO/IEC TR 133353: 1998. Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI.
[4] ISO/IEC 133354: 2000. Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas.

ASOCOLFLORES G.M. Secretario General

[5] ISO 14001:2004. Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso.
[6] ISO/IEC TR 18044:2004.Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información.