POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACION

CONTENIDO

INTRODUCCIÓN

La Cámara de Comercio de Pasto decide implementar las políticas de seguridad informática con el propósito de cumplir sus mayores objetivos definidos a través de componentes confiables, íntegros y seguros. En primer lugar, es necesario reconocer que la información es uno de los elementos más importantes y valiosos dentro de una empresa, a través de ella, proporciona herramientas necesarias para la toma de decisiones, retroalimentar y mejorar la estructura interna de la organización bajo un uso adecuado.

Cada día nos enfrentamos a nuevas modalidades y técnicas de ataques informáticos que acceden, sin el consentimiento del propietario a todo activo de información, no obstante, es importante reconocer que también hay acciones preventivas y correctivas que contrarrestan este hecho; lo más importante es conocerlos y aplicarlos en el momento adecuado.

Este manual pretende dar a conocer las políticas de seguridad con el mayor objetivo de llevar su implementación en conjunto y de forma coordinada. Se establece como base de referencia la norma ISO 27001 y 27002 de la seguridad de la información la cual pretende establecer, preservar, mantener la integridad y disponibilidad de la información basados en puntos de control analizados dentro de la Cámara de Comercio de Pasto.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

El objetivo general del manual de gestión de seguridad informática y seguridad de la información es brindar a las unidades y a los usuarios de tecnologías de información de la Cámara de Comercio de Pasto, un conjunto de lineamientos e instrucciones que permiten garantizar la seguridad en el ambiente informático, la información y demás recursos tecnológicos.

1.2. OBJETIVOS ESPECÍFICOS

- Promover el uso de las mejores prácticas de seguridad informática en el área de trabajo.
- Implementar los mecanismos de seguridad informática de modo que propicie la confidencialidad, integridad y disponibilidad de la información.
- Guiar el comportamiento profesional y personal de los funcionarios de la Cámara de Comercio de Pasto, en procura de minimizar los incidentes de seguridad internos.
- Implementar prácticas de seguridad que permitan la correcta custodia de los datos y equipos administrados por los líderes de cada departamento en la Cámara de Comercio de Pasto.
- Verificar el cumplimiento de aspectos legales y técnicos en materia de seguridad informática.
- Homologar la forma de trabajo de personas de diferentes unidades y situaciones que tengan responsabilidades y tareas similares.

2. ALCANCE

El alcance del sistema de gestión de seguridad informática y de la información en la Cámara de Comercio de Pasto está enfocado principalmente en todos los elementos de control ejecutados por los directivos, funcionarios, terceros, clientes e invitados.

3. CONCEPTOS GENERALES

3.1. ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La información es un activo importante, tiene valor para la organización y por lo tanto requiere una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la empresa y maximizar el uso de los recursos informáticos.

La información en sus diversas formas, presentaciones y divulgaciones debería ser protegida adecuadamente a partir del momento que se crea, almacene y comparta.

La seguridad de la información se caracteriza aquí como la preservación de:

a) Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.

b) Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.

c) Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

3.2.¿PORQUÉ ES NECESARIA LA SEGURIDAD DE INFORMACIÓN?

La información, los procesos que la apoyan, los sistemas y redes son completamente indispensables. La disponibilidad, integridad y confidencialidad son esenciales para mantener su competitividad, rentabilidad y cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Para la Cámara de Comercio de Pasto es importante implementar la seguridad de la información con el fin de mantener su integridad brindando un servicio confiable, a todos los clientes que requieren una solución acorde a sus necesidades.

4. GENERALIDADES SOBRE SEGURIDAD INFORMÁTICA.

Se define los sistemas de información como "el conjunto de recursos (datos, personas, instalaciones, equipamientos y software) que, en forma coordinada y alineada a una estrategia institucional, proporcionan soporte a la operación, a la toma de decisiones y al servicio de los usuarios de la organización como a sus clientes"

La información provista y las tecnologías de la información (TI) que los soportan, representan inversiones valiosas para la Cámara de Comercio de Pasto, por lo que la administración priorizó las expectativas respecto a la función de las áreas de servicios informáticos, como áreas de soporte a las funciones de la Organización y sujeto de control sobre sus responsabilidades y bienes asignados, para lograr incrementar la productividad, funcionalidad y facilidad de uso, disminuyendo el tiempo de entrega, y aumentando continuamente los niveles de servicio en el paradigma de la calidad, con la premisa que todo esto se logre con menores costos y con la administración de los riesgos asociados a la implementación de nuevas tecnologías de información.

Toda organización se encuentra sometida a amenazas o peligros de diversos orígenes, desde un posible incendio casual o intencional hasta la defraudación, pasando por la más común de las amenazas; el error u omisión cometidos por las personas en el normal desenvolvimiento de sus tareas.

Las organizaciones pueden estar o no ordenadamente preparadas para enfrentar los peligros o amenazas latentes. Este aspecto es el que en la Cámara de Comercio de Pasto denominamos vulnerabilidad y representa las debilidades que la organización presenta frente a cada una de las eventuales amenazas.

Por los motivos expuestos, los responsables de los sistemas de información y sus tecnologías relacionadas, como así los responsables de la función servicios informáticos, necesitan tener el conocimiento de las nuevas amenazas a que se ven sometidos los organismos por el uso de las tecnologías de la información, como así también de los elementos de control que permiten minimizar o eliminar las mismas, a través de una administración efectiva que permita vincular las amenazas, mecanismos de control y las tecnologías, para minimizar o eliminar el riesgo asociado.

Los controles relacionados a la seguridad se establecen para impedir el acceso físico y lógico a los sistemas de información y sus recursos relacionados por parte de personas que no tienen autorización, como también ayuda a reducir el riesgo de que las personas autorizadas cambien o destruyan accidentalmente los datos.

Los controles se establecen mediante la implementación de un conjunto de medidas preventivas, disuasivas y correctivas, destinadas a proteger aspectos como la disponibilidad, integridad, confidencialidad y privacidad.

5. MARCO LEGAL

- COBIT: (Control Objectives for Information Systems and related Technology) Conjunto de Buenas prácticas que promueve objetivos de control para la información y la tecnología. COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

- DECRETO 1474 DE 2002 (Julio 15): Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)".

- ISO IEC 27001-2005: Estándares internacionales sobre tecnología de la información, técnicas de seguridad, Administración de seguridad de la información, los cuales proporcionan un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de empresa.

- ITIL: (Information Technology Infrastructure Library) Marco de trabajo de mejores prácticas para el manejo de servicios de TI.

- Ley 1273 de 5 de enero de 2009: Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones.

- Ley 1712 del 6 de marzo de 2014: Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones

- Ley 44 DE 1993 (febrero 5): por la cual se modifica y adiciona la Ley 23 de 1982 Sobre derechos de autor.

- Ley Estatutaria 1581 De 2012: Protección de los datos personales (Habeas data)

6. POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

6.1. POLÍTICA GENERAL

La Presidencia de La Cámara de Comercio de Pasto, apoya los objetivos y principios de la seguridad informática y de la información para lo cual se determina el obligatorio conocimiento y cumplimiento de la reglamentación y políticas de seguridad informática de la empresa consignadas en el presente manual.

El acatamiento de las directrices y políticas definidas a continuación evita incurrir en posibles sanciones y/o perjuicios tanto a la empresa como a los funcionarios y contratistas.

"TODO AQUELLO QUE NO SE AUTORICE EN FORMA EXPRESA, ESTÁ PROHIBIDO"

El Manual de Políticas de Seguridad Informática y de la Información deberá ser divulgado a todos los funcionarios y contratistas vinculados con la Cámara de Comercio de Pasto a través de cualquier medio que posea actualmente y que asegure su entrega.

El comité de seguridad podrá, en el momento que lo considere apropiado, modificar, remover o añadir las Políticas de Seguridad de la Información que conforman la Cámara de Comercio de Pasto.

6.2. POLÍTICA PARA VINCULACIÓN DE FUNCIONARIOS

La Cámara de Comercio de Pasto tiene a consideración los recursos humanos para el cumplimiento de sus objetivos. Con el fin de contar con el personal idóneo, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

6.2.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO RELACIONADAS CON LA VINCULACIÓN DE FUNCIONARIOS

- El área de Gestión Humana debe certificar que los funcionarios de la empresa firmen una Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

- El funcionario provisto por terceras partes, deben garantizar el cumplimiento de la Cláusula de Confidencialidad y aceptación de las Políticas de Seguridad de la Información.

6.3. POLÍTICA QUE CONTEMPLA LICENCIAS, DESVINCULACIÓN, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

La Cámara de Comercio de Pasto debe asegurar de forma controlada y segura la desvinculación o reasignación del personal para la ejecución de nuevas labores.

6.3.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA LA DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIOS DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

- El área de Gestión Humana debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la empresa llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

- El área de Gestión Humana debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a El área de Gestión Tecnológica.

- El área de Gestión Tecnológica debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

6.4. POLÍTICA PARA EL ACCESO Y SEGURIDAD DE LAS ÁREAS FÍSICAS DONDE SE ENCUENTREN RECURSOS INFORMÁTICOS

Las áreas de la empresa relacionadas directa o indirectamente con el procesamiento o almacenamiento de información de la empresa, así como aquellas en las que se encuentren equipos e infraestructura de soporte a los sistemas de información y comunicaciones, se considerarán como áreas de acceso restringido y por lo tanto se deben implementar medidas de control de acceso del personal a dichas áreas.

La Cámara de Comercio de Pasto deberá contar con los mecanismos de control de acceso a los ambientes físicos donde se encuentren recursos informáticos, tales como puertas de seguridad, sistema de alarmas y circuitos cerrados de televisión en los lugares que la empresa considere críticas.

6.4.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA EL ACCESO Y SEGURIDAD DE LAS ÁREAS FÍSICAS DONDE SE ENCUENTREN RECURSOS INFORMÁTICOS

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios que pertenecen al Área de Gestión Tecnológica. Los visitantes siempre deberán estar acompañados de un funcionario de dicha área durante su visita al centro de cómputo o a los centros de cableado.

- El área de Gestión Tecnológica debe registrar la entrada de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia.

- El área de Gestión Tecnológica debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

- Los funcionarios deben portar el carné en un lugar visible mientras se encuentren en las instalaciones de la empresa; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

- Los funcionarios de la Cámara de Comercio de Pasto y aquellos que tengan a cargo terceras partes no deben ingresar a ubicaciones a las cuales no tengan autorización.

6.5. POLÍTICA PARA LA RESPONSABILIDAD DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de la Cámara de Comercio de Pasto realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

6.5.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA LA RESPONSABILIDAD DE ACCESO DE LOS USUARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la Cámara de Comercio de Pasto deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes a menos que haya una justificación que lo amerite; dado el caso se realizará un análisis de esta causa con el superior directo, el área de Control Interno y el área de Gestión Tecnológica.

- Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la empresa deben acogerse a lineamientos para la configuración de contraseñas implantados por la Cámara de Comercio de Pasto.

6.6. POLÍTICA PARA USO DE MEDIOS DE ALMACENAMIENTO Y PERIFÉRICOS

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la Cámara de Comercio de Pasto será reglamentado por El área de Gestión Tecnológica, considerando las labores realizadas por los funcionarios y su necesidad de uso.

6.6.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA USO DE MEDIOS DE ALMACENAMIENTO Y PERIFÉRICOS

- El área de Gestión Tecnológica debe establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Cámara de Comercio de Pasto.

- El área de Gestión Tecnológica debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la empresa, de acuerdo con los lineamientos y condiciones establecidas.

- El área de Gestión Tecnológica debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la empresa, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

- El área de Gestión Tecnológica debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la empresa de acuerdo con el perfil del cargo del funcionario solicitante.

- Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por El área de Gestión Tecnológica.

- Los funcionarios de la Cámara de Comercio de Pasto y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por El área de Gestión Tecnológica.

- Los funcionarios y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados.

- Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la Cámara de Comercio de Pasto.

- El área de Gestión Tecnológica debe generar y publicar un instructivo que plasme las buenas prácticas de uso de medios de almacenamiento para la prevención de riesgos.

6.7. POLÍTICA DE ACCESO A REDES Y SUS RECURSOS

El área de Gestión Tecnológica de la Cámara de Comercio de Pasto, está a cargo de las redes de datos y los recursos de red, dichas redes deben estar protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

6.7.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE ACCESO A REDES Y RECURSOS

- El área de Gestión Tecnológica debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Cámara de Comercio de Pasto.

- El área de Gestión Tecnológica debe asegurar que las redes inalámbricas de la empresa cuenten con métodos de autenticación que eviten accesos no autorizados.

- El área de Gestión Tecnológica debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de la Cámara de Comercio de Pasto.

- Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la Cámara de Comercio de Pasto, deben contar con el

formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la empresa deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

6.8. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

La Cámara de Comercio de Pasto, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

6.8.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE USO DEL CORREO ELECTRÓNICO

- El área de Gestión Tecnológica debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

- El área de Gestión Tecnológica debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

- El área de Gestión Tecnológica debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la empresa o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya a menos que haya una justificación que lo amerite.

- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Cámara de Comercio de Pasto. El correo institucional no debe ser utilizado para actividades personales.

- Los mensajes y la información contenida en los buzones de correo son propiedad de la Cámara de Comercio de Pasto y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Los usuarios de correo electrónico institucional tienen prohibido la remisión de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la empresa y el personal provisto por terceras partes.

- No se permite el envío de archivos que contengan extensiones ejecutables.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Cámara de Comercio de Pasto y deben conservar en todos los casos el mensaje legal corporativo.

6.9. POLÍTICA DE USO ADECUADO DE INTERNET

La Cámara de Comercio de Pasto consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la empresa.

6.9.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE USO ADECUADO DE INTERNET

- El área de Gestión Tecnológica debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

- El área de Gestión Tecnológica debe monitorear continuamente el canal o canales del servicio de Internet.

- El área de Gestión Tecnológica debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

- Los usuarios del servicio de Internet de la Cámara de Comercio de Pasto deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este manual.

- No está permitido 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 entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y El área de Gestión Tecnológica, 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.

- No está permitido el intercambio no autorizado de información de propiedad de la Cámara de Comercio de Pasto, de sus clientes y/o de sus funcionarios, con terceros.

6.10. POLÍTICA SOBRE POLÍTICA EDITORIAL Y DE ACTUALIZACIÓN DE LA INFORMACIÓN EN LA PÁGINA WEB

La información publicada en la página web de la empresa debe ser actualizada permanentemente y además será objetiva, clara, imparcial, sin emisión de juicios de valor, veraz, institucional, accesible y confiable para la consulta tanto de los usuarios internos como externos de la empresa.

La información publicada en la página web de la empresa deberá mantener un formato y un estilo constante, con fuentes de información claramente definidas y confiables que serán presentadas en concordancia con la plataforma estratégica de la empresa y las políticas de comunicación y seguridad informática.

6.10.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO SOBRE POLÍTICA EDITORIAL Y DE ACTUALIZACIÓN DE LA INFORMACIÓN EN LA PÁGINA WEB

- La información publicada en la página web de la empresa será entregada por cada una de las dependencias responsables de los procesos generadores de la misma, con revisión y aprobación del jefe o líder del proceso y a su vez por el área de Comunicación.

- El administrador de la Página Web de la empresa será el responsable y compartirá las funciones de actualización de los datos y contenidos de las diversas secciones de la página, junto con el responsable de su edición. Dicha actualización se realizará simultáneamente al proceso de publicación, cuando sea necesaria o se presente alguna novedad.

- La Página Web de la empresa podrá contar con enlaces hacia otros sitios Web, cuando se considere que estos son útiles y de relevancia bien sea para comunidad en general o para el personal del sector cameral. Una vez que el usuario acceda a otro portal a través de un link almacenado en la página web de Cámara de Comercio de Pasto, estará sujeto a la política de privacidad y a la política editorial del portal nuevo.

- Los derechos de propiedad intelectual de cualquier material presentado en la Página Web de la empresa, incluyendo textos, fotografías, otras imágenes, sonidos y otros, son de propiedad de sus autores, incluyendo a la Cámara de Comercio de Pasto, así se reservan todos los derechos de propiedad intelectual sobre los contenidos de su autoría y sobre las que sean cedidas.

6.11. POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Cámara de Comercio de Pasto a través de la Oficina de Riesgos, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la Cámara de Comercio de Pasto, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la Camara de Comercio de Pasto, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la Cámara de Comercio de Pasto exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la Camara de Comercio de Pasto conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la empresa y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

6.11.1. Instrucciones de obligatorio cumplimiento de privacidad y protección de datos personales

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la empresa.

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las empresas vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos

para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

- Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la empresa o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

- Es deber de los usuarios, verificar la identificación de la empresa de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

6.12. POLÍTICA PARA USO DE TERMINALES MÓVILES

La Cámara de Comercio de Pasto suministrará las condiciones para el manejo de los dispositivos móviles institucionales y personales que hagan uso de los servicios de la empresa.

6.12.1. Instrucciones de obligatorio cumplimiento para uso de dispositivos móviles

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

- El área de Gestión Tecnológica debe establecer las configuraciones aprobadas para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la Cámara de Comercio de Pasto.

- El área de Gestión Tecnológica debe implementar un método de bloqueo para los dispositivos móviles institucionales que serán entregados a los usuarios.

- El área de Gestión Tecnológica debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y salvaguardar estos códigos en un lugar seguro.

6.13. POLÍTICA PARA CONEXIONES REMOTAS

La Cámara de Comercio de Pasto establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la empresa; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

6.13.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA USO DE CONEXIONES REMOTAS

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Cámara de Comercio de Pasto y deben acatar las condiciones de uso establecidas para dichas conexiones.

- El área de Gestión Tecnológica debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la Cámara de Comercio de Pasto.

- El área de Gestión Tecnológica debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la Cámara de Comercio de Pasto.

- El área de Control Interno debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica de la Cámara de Comercio de Pasto.

6.14. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

La Cámara de Comercio de Pasto velará porque la información de la empresa, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

6.14.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE CONTROLES CRIPTOGRÁFICOS

- El área de Gestión Tecnológica debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

- El área de Gestión Tecnológica debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

6.15. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

La Cámara de Comercio de Pasto proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

6.15.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

- El área de Gestión Tecnológica debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Cámara de Comercio de Pasto y los servicios que se ejecutan en la misma.

- El área de Gestión Tecnológica debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

- El área de Gestión Tecnológica debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

- El área de Gestión Tecnológica, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

- El área de Gestión Tecnológica, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por El área de Gestión Tecnológica; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al área de Gestión Tecnológica tome para tomar medidas de control pertinentes.

6.16. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La Cámara de Comercio de Pasto autenticará la generación de copias de respaldo y almacenamiento de su información importante, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de El área de Gestión Tecnológica, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

6.16.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE COPIAS DE RESPALDO DE LA INFORMACIÓN

- El área de Gestión Tecnológica, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

- El área de Gestión Tecnológica debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

- El área de Gestión Tecnológica, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

- El área de Gestión Tecnológica debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

- Es responsabilidad de los usuarios de la plataforma tecnológica de la Cámara de Comercio de Pasto identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

6.17. POLÍTICA SOBRE CONTINUIDAD DEL FUNCIONAMIENTO DE LOS SISTEMAS DE INFORMACIÓN Y RECURSOS INFORMÁTICOS

La Empresa debe contar con un plan de contingencia que permita dar continuidad al funcionamiento de sus sistemas de información y a sus recursos informáticos, garantizando su disponibilidad en el evento de una emergencia o desastre como terremoto, erupción volcánica, terrorismo, inundación, robo etc. Este plan de contingencia deberá socializarse en toda la empresa, deberá actualizarse y probarse periódicamente para que se aplique en el evento en que se ponga en riesgo la continuidad de los sistemas de información o el funcionamiento de los recursos informáticos.

6.17.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA LA CONTINUIDAD DEL FUNCIONAMIENTO DE LOS SISTEMAS DE INFORMACIÓN Y RECURSOS INFORMÁTICOS

- El área de Gestión de la Información y el área de Control interno deben realizar un plan de contingencia para la continuidad de negocio dentro de la Cámara de Comercio de Pasto.

7. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instaurar y consolidar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de la Cámara de Comercio de Pasto. Por tal razón, es necesario que los desacatos a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo a las circunstancias.

GLOSARIO

Entiéndanse para el presente documento los siguientes términos:

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

Acuerdo de Confidencialidad: es u documento en los que los funcionarios de la Cámara de Comercio de Pasto o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la empresa, 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.

Amenaza: Es el conjunto de los peligros a los que están expuestos los sistemas de información y sus recursos tecnológicos relacionados, los que pueden ser de tipo accidental o intencional.

Amenaza Accidental: Cuando no existe un deliberado intento de perjudicar a la organización.

Amenaza Intencional: Su móvil es perjudicar a la organización u obtener beneficios en favor de quien comete la acción.

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.

Ataque cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

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

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.

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.

Certificado Digital: Es un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Cifrar: Se refiere a transformar un mensaje en un documento no legible, y el proceso contrario se llama "descodificar" o "descifrar". Los sistemas de cifrado se llaman sistemas criptográficos".

Confidencialidad: Asegurar que los sistemas de información y sus recursos relacionados sean solo accedidos por los funcionarios o contratistas de Cámara de Comercio de Pasto, basados en la necesidad de saber o de hacer de sus cargos.

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

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

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Criptografía de llave publica: Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

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.

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución 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 consecuencias, el número de veces ocurrido o el origen (interno o externo).

Información: Existe de varias formas. Puede estar impresa en papel, almacenada electrónicamente, transmitida por correo electrónico o utilizando medios magnéticos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Integridad: es la protección de la exactitud y estado completo de los activos.
Integridad: Exactitud y plenitud de los sistemas de información y sus recursos relacionados, limitando la gestión sobre los mismos a personas autorizados y programas de aplicación aprobados y autorizados, protegiéndolos contra pérdida, destrucción o modificaciones accidentales o intencionales.

Keylogger: Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Licencia de software: es un contrato en donde se especifican todas las Instrucciones de obligatorio cumplimiento 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.

Phishing: Es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc.
Política: Son instrucciones que indican la intención de La Presidencia respecto a la operación de la organización respecto a un asunto determinado.
Procesos informáticos: Son los procesos que tienen relación directa con los servicios que se prestan a los usuarios de los sistemas de información y sus tecnologías relacionadas, procesos que consisten en tomar un insumo, agregarle valor y generar un producto que satisface a un cliente interno o externo.

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.
Recurso Informático: Elementos electrónicos digitales (base de datos, sistemas operacionales, redes, equipos de cómputo, sistemas de información y comunicaciones) que facilitan servicios informáticos.

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 la Cámara de Comercio de Pasto.

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la empresa. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

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.

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.
Spam: Se llama spam, al correo basura o a los mensajes no solicitados, no deseados o de remitente desconocido.

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

TI: Tecnología de la Información.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios o contratistas de Cámara de Comercio de Pasto, pero que por las actividades que realizan en la Entidad, deban tener acceso a recursos Informáticos.

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 la Cámara de Comercio de Pasto (amenazas), las cuales se constituyen en fuentes de riesgo.

Web Proxy: Un proxy o servidor proxy, en una red informática, es un servidor programa o dispositivo, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).