

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

1. OBJETIVO:

Establecer los lineamientos a seguir en relación con la seguridad informática de la Cámara de Comercio de Urabá, tanto para equipos como para los diferentes programas y aplicaciones que se utilizan en la prestación del servicio, de tal manera que se controlen o minimicen los accesos no deseados y se preserve la información y su respectiva privacidad.

2. ALCANCE:

Este procedimiento se aplica para la creación, modificación y eliminación de usuarios y claves de respaldo, permisos para los diferentes programas y aplicaciones, manejo de copias de seguridad de la información y seguridad informática en general para la **CÁMARA DE COMERCIO DE URABÁ**.

3. CONDICIONES GENERALES:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar las políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia de la Cámara de Comercio y Líder de TI.

Existen lineamientos a cerca del acatamiento de políticas de operación en materia de:

- Uso de recursos informáticos.
- Uso de contraseñas.
- Uso de la información.
- Uso de Internet y correo electrónico.
- Uso de la Intranet y Sitio Web de la Cámara de Comercio
- Manejo de la información hacia externos.
- Selección de información para efectuar copias de respaldo.
- Uso de Firewall.
- Políticas para Usuarios externos.
- Políticas de acceso físico
- Uso de portátiles.

La infraestructura de TI de la Cámara de Comercio de Urabá está compuesta de la siguiente manera:

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

Canal a Internet: Cuenta con dos (2) canales dedicado a Internet, uno de 60 Mb suministrado por la empresa Une-Tigo, con una dirección IP pública válida y canal dedicado de 25 Mb suministrado por la empresa COMTIC S.A.S como contingencia.

Firewall: Se tiene un Appliance DELL SonicWALL TZ400 y un SonicWALL Tz 210 como contingencia que provee los servicios y es la única máquina visible desde Internet, hace las veces de puerta de enlace por ende todo el tráfico desde dentro hacia fuera, y viceversa debe pasar a través de él. En el Firewall se encuentra configurado el DNS del proveedor ISP y los logs.

Hosting de Página Web: Servicio en la nube proveído por la empresa estadounidense Hostmonster. Este Hosting tiene alojado el siguiente dominio: www.ccuraba.org.co: Página institucional de la Cámara de Comercio de Urabá.

Correo: El correo empresarial se maneja a través de Microsoft office365 que usa Exchange Server. Se tiene una cuenta de administrador manejada por el jefe de sistemas para crear y eliminar cuentas de correo y configuraciones avanzadas.

Servidor Registros Públicos: Es un servidor Virtual alojado en la plataforma de AMAZON a través de CONFECAMARAS. Este servidor es utilizado como Aplicación SII, encargado de la gestión de los Registros Públicos y registros virtuales delegados por el estado (SII – Sistema Integrado de Información – Registros públicos virtuales y Proponentes), el cual se integra (interoperabilidad) con otras plataformas a través de APIs.

Servidor de Imágenes: Servidor en nube a través del proveedor Makrosoft donde se opera el programa de Gestión documental (Docxflow), con almacenamiento de max 400 gb dedicado a imágenes. Este servidor procesa y almacena la información documental de los Registros Públicos de la organización en formato PDF, que se gestionan a través del Software DocxFlow de la firma MAKROSOFT y que se integra con el sistema de Registros públicos (SII).

Servidor de Dominio y Archivos: Se ha habilitado una máquina SURE, con un procesador Pentium IV de 1.80 Ghz y 704 MB de RAM Sistema Operacional Windows Server y disco de 500 GB.

Este servidor almacena la información de todas las áreas de la institución referente a los archivos de manejo y funcionamiento del área (documentos de Word, archivos de Excel y Presentaciones de Power point entre otros).

Este servidor se utiliza únicamente para aplicaciones internas.

- Controlador de Dominio: El dominio CAMARA controla los accesos de los usuarios y los en ruta a las Carpetas donde tienen permisos de acceso.

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

- DNS: (servicio de Nombres de Dominio) Traduce los nombres de dominio y dns de equipo en direcciones IP.
- WINS: (servicio de nombres de internet de windows) Traducen nombres de equipo y NetBios de dominio en direcciones IP.

DVR Cámaras de Vigilancia: Se tiene ha habilitado una DVR iVMS-4200 con capacidad de almacenamiento de 4TB y permite monitorearse a través de la WEB.

Servidor de Antimalware Cloud: Se tiene instalado un antivirus central de la firma CISCO (fireAMP), que utiliza una consola de administración de donde se configuran los clientes y las actualizaciones.

Sistema Eléctrico y de Respaldo mediante UPS: Comprende el siguiente esquema.

- Circuito eléctrico del Área de Sistemas. Los servidores, Switches, Enrutadores, Firewall y módems de Internet se encuentran en un circuito eléctrico de energía acondicionada y regulada por UPS de 10 KVA con 24 baterías de 12 V (voltios); lo que nos permite una autonomía aproximada de 35 minutos, suficiente debido al cambio automático de corriente de la planta eléctrica del edificio.
- Circuito eléctrico para 30 PC (usuarios internos). Estos están regulados por la misma UPS de 10 KVA con 24 baterías de 12 V (voltios); lo que nos permite una autonomía aproximada de 35 minutos, suficiente debido al cambio automático de corriente de la planta eléctrica del edificio
- Circuito no regulado. En el cual se conectan las impresoras, lo escáneres, teléfonos inalámbricos. Este circuito no está regulado pero si acondicionado, posee un tablero de control independiente; el cual está soportado por un acondicionador de 50 Kilovatios alojado en la subestación del edificio.
- Planta Eléctrica: CATERPILLAR 3406C GENERATOR SET C2Y01671. Capacidad de 350 KVA, trifásica con transferencia automática alojada en la planta baja del edificio y espacio con sistema insonorización.

Centro de Cómputo: Cuenta con un área aproximada de 30 mts². Esta área posee las siguientes características:

- Contiene los tableros de control de las UPS
- Contiene RACK de Cableado Estructurado(red cat. 7^a)
- Contiene RACK para los servidores. Allí están aglomeradas todas las torres.

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

- Contiene una consola de administración (KVA) a través de la cual se administran 2 servidores a través de una pantalla un teclado y un mouse.
- Cuenta con 2 Aires Acondicionado tipo Multi-Split de 12.000 y 24.000 BTU.
- Oficinas del jefe de sistemas y soporte técnico.

4. DEFINICIONES:

Para los propósitos de este documento se aplican los siguientes términos y definiciones:

Activo: Cualquier bien que tenga valor para la organización.

Acuerdo de Confidencialidad: Documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de la Cámara de Comercio.

Administradores: Usuarios a quienes se les ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la entidad, quienes estarán bajo el control del Coordinador de Sistemas.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Backup: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Directrices: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

Servicios de procesamiento de la información: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

Evento de seguridad de la información: Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Firewall: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.

Incidente de seguridad de la información: Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de la Cámara de Comercio y amenazar la seguridad de la información.

Información confidencial (RESERVADA): Información administrada por la Cámara de Comercio en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.

Información confidencial (CONFIDENCIAL): Información generada por la Cámara de Comercio en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

Información privada (USO INTERNO): Información generada por la Cámara de Comercio en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.

Información pública: Es la información administrada por la Cámara de Comercio en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo, la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES. LAN: Grupo de computadores y dispositivos asociados que

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio ó una oficina).

Licencia de Software: Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.

Copyright: Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, s radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.

Propiedad Intelectual: Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.

Open Source (Fuente Abierta): Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.

Shareware: Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago económico.

Módem (Modulador - Demodulador de señales): Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.

Monitoreo: Verificación de las actividades de un usuario con respecto a los recursos informáticos de la Cámara de Comercio.

OTP (One Time Password): Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

Plan de contingencia: Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de la Cámara de Comercio en casos de desastres y otros casos que impidan el funcionamiento normal.

Política: Toda intención y directriz expresada formalmente por la Dirección.

5. CONTENIDO:

	ACTIVIDAD	RESPONSABLE	REGISTRO
5.1	CREAR, MODIFICAR Y/O ELIMINAR USUARIOS: Cuando una persona ingresa nueva a la Cámara, el líder del proceso correspondiente solicita al Jefe de TI la creación de su usuario y clave para ingreso a los sistemas de la entidad. TI crea el usuario y contraseña con las especificaciones y permisos respectivos, según los procesos en los que participará el nuevo empleado. De la misma manera, cuando por alguna razón se requiera hacer una modificación o eliminación de usuario ya existente, el líder del proceso, solicita este trámite al líder de TI para su ejecución. TI informa, cuando termina dicha actividad, al usuario del sistema y/o al líder de proceso, con el fin de que esta persona verifique en el sistema y haga el ingreso correspondiente para corroborar la funcionalidad de la misma, en caso de tener alguna dificultad, lo notifica a TI para su corrección y adecuación.	Líder de TI	FTI02 – Control de Usuarios de TI

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

	El usuario cuando ingresa por primera vez establece su propia clave, teniendo en cuenta las directrices de cantidad de caracteres y que sea alfanumérica. TI lleva registro de los usuarios en el Formato FTI02 – Control de Usuarios.		
5.2	CONTROLAR LAS CLAVES DE ACCESO: Cada usuario es responsable de controlar su propio usuario y clave de acceso, ya que es personal e intransferible, por lo cual las transacciones que se realicen en los diferentes sistemas de la Cámara mediante su contraseña, son su responsabilidad. Teniendo en cuenta lo anterior, es por esto que se deben cumplir las directrices de manejo de usuarios y contraseñas como lo especifica el presente procedimiento.	Usuario	Monitoreo del manejo de claves (en el sistema)
5.3	ADMINISTRAR CLAVES DE ACCESO: Según el programa o aplicación de la Cámara, el usuario debe administrar su contraseña, así: Para el sistema de Registros Públicos, la clave debe ser cambiada directamente por cada usuario cada 15 días, el sistema está programado automáticamente para que solicite cambio de clave en ese lapso de tiempo. El sistema registral envía la clave al correo de la persona para que ella la aplique y así quede modificada.	Usuario	Monitoreo del manejo de claves (en el sistema)

	PROCEDIMIENTO SEGURIDAD INFORMÁTICA	Código: PTI02 Versión: 02
		Fecha: Noviembre 15 de 2020

5.5	SEGURIDAD INFORMÁTICA: En la Cámara de Comercio de Urabá se tiene restricción para el uso de páginas web que no se requieran para la realización del trabajo, dado que es importante tener en cuenta los virus que se pueden adquirir a través de éstas y que pueden ser perjudiciales para la información contenida en los diferentes equipos o servidores. De la misma manera, como se menciona anteriormente, cada usuario es responsable de sus claves de seguridad para garantizar el manejo adecuado de cada uno de los módulos de los diferentes programas, así como la coherencia y preservación de la información.	Usuario	Acceso a páginas y programas
------------	---	---------	------------------------------

ELABORÓ: Contratista Asesor SCCI	REVISÓ: Líder de TI	APROBÓ: Eladio Ramírez Vásquez
-------------------------------------	------------------------	-----------------------------------

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
01	30 de junio de 2018	Elaboración del documento en el Sistema documental
02	15 de noviembre de 2020	Ajustes al contenido del documento