RESOLUCIÓN No.026
31 de julio de 2018

"Por medio del cual se actualiza la política de Sistemas de información y tecnología"

El Presidente Ejecutivo de **LA CÁMARA DE COMERCIO DE OCAÑA**, en uso de sus atribuciones legales estatutarias y

CONSIDERANDO

Que **LA CÁMARA DE COMERCIO DE OCAÑA**, es una organización privada, de carácter gremial, sin ánimo de lucro, con personería jurídica reconocida mediante el Decreto No. 1744 del 29 de mayo de 1986 expedido por el Gobierno Nacional, que representa al sector empresarial y a la comunidad en general.

Que **LA CÁMARA DE COMERCIO DE OCAÑA**, cumple eficazmente con las funciones delegadas por el gobierno; trabaja con motivación y dinamismo generando espacios de asociatividad y apoyando de manera integral a los empresarios para el cabal cumplimiento de su compromiso con la región.

Que es deber de la Presidencia Ejecutiva de **LA CÁMARA DE COMERCIO DE OCAÑA**, establecer lineamientos para el fortalecimiento de los procesos de la Institución.

Que La Ley 1273 de 2009 adiciona al código penal "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y comunicaciones.

Que la Ley 1581 de 2012 y decreto reglamentario de 1377 de 2013 se expidió el régimen nacional de protección de datos personales

Que según la Resolución 050 la Cámara de Comercio adopto el manual de Políticas y procedimientos para la protección de datos personales.

Que es deber de los funcionarios de la Entidad aplicar las políticas en la implementación de los procesos y actividades de control.

Que en virtud de lo anterior expuesto,

RESUELVE

CAPÍTULO PRIMERO
DISPOSICIONES GENERALES

ARTÍCULO PRIMERO. OBJETO: El activo más valioso de la Cámara de Comercio de Ocaña, es la información recolectada en los diferentes Registros públicos, no solo aquella que hace parte de estos registros y es suministrada por los comerciantes, sino la que se genera por el mismo cumplimiento de la labor encomendada por el Estado Colombiano, es por esto que se hace necesario brindar a usuarios internos y externos de la Cámara de Comercio de Ocaña un conjunto de lineamientos e instrucciones que permiten garantizar la seguridad en el ambiente informático, la información y demás recursos tecnológicos.

De igual forma se debe promover el uso de las mejores prácticas de seguridad informática en el área de trabajo, implementando estos mecanismos que propicien la confidencialidad, integridad y disponibilidad de la información, para que de esta forma se pueda guiar el comportamiento profesional y personal de los funcionarios de la Cámara de Comercio de Ocaña, en procura de minimizar los incidentes de seguridad internos, situación esta que se complementa con la implementación de prácticas de seguridad que permitan la correcta custodia de los datos y equipos administrados por los diferentes usuarios de la Cámara de Comercio de Ocaña, verificando el cumplimiento de aspectos legales y técnicos en materia de seguridad informática.

ARTÍCULO SEGUNDO. ALCANCE: El documento de política de Sistemas de información y tecnología reglamenta la protección y uso de los activos de información de la Cámara de Comercio, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos; Estos usuarios pueden ser usuarios internos o externos.

Usuarios internos: Son todos aquellos usuarios que han celebrado algún tipo de contrato laboral, orden de trabajo, práctica profesional o pasantía con la Cámara de Comercio de Ocaña y tengan contacto con los activos de la información de la Entidad.

Usuarios Externos: son aquellos usuarios que no están vinculados con la Cámara de Comercio y que previa solicitud acceden a la información de la entidad; estos pueden ser entidades de control o usuarios que estén inscritos o no en los registros públicos que lleva la Cámara de Comercio de Ocaña.

CAPITULO II
DEFINICIONES

ARTÍCULO TERCERO.

Activo: Cualquier bien que tenga valor para la organización.
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.
Contraseña: Clave de acceso a un recurso informático.
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.
Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.

Firewall: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.
Freeware: Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.
Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
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 del negocio y amenazar la seguridad de la información.
Información: Datos relacionados que tienen significado para la organización. Además, es un activo que, como otros activos importantes de la entidad, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad 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.
Integridad: Salvaguardia de la exactitud y completitud de la información y sus métodos de procesamiento.
LAN: Grupo de computadores y dispositivos asociados que 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.
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 especifica el uso que se le puede dar al software.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
Software Libre: Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.
Software pirata: Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.
Software de Dominio Público: Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
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.
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.

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.

Protector de pantalla: Programa que se activa a voluntad del usuario, ó automáticamente después de un tiempo en el que no ha habido actividad.

Recursos informáticos: Son aquellos elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Router: Equipo que permite la comunicación entre dos o más redes de computadores.

Sesión: Conexión establecida por un usuario con un Sistema de Información.

CAPITULO III
POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

ARTÍCULO CUARTO. POLÍTICA GENERAL

La Cámara de Comercio de Ocaña, 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, contempladas en la presente resolución.

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"

Las políticas de los sistemas de información y tecnología deberá ser divulgado a todos los funcionarios y contratistas vinculados con la Cámara de Comercio de Ocaña a través de cualquier medio que posea actualmente y que asegure su entrega.

La Dirección de Sistemas podrá, en el momento que lo considere apropiado, modificar, remover o añadir Las políticas de los sistemas de información y tecnología que conforman la Cámara de Comercio de Ocaña

ARTICULO QUINTO. POLÍTICA PARA VINCULACIÓN DE FUNCIONARIOS

La Cámara de Comercio de Ocaña 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.

En este orden de ideas a la Dirección de Sistemas se le debe informar que recursos tecnológicos e informáticos se le deben asignar al nuevo funcionario, junto con los usuarios y perfiles que deben asignársele en los sistemas informáticos que éste vaya a utilizar.

Cuando un usuario inicie su relación laboral con La Cámara de Comercio se debe diligenciar el documento de entrega de equipos tecnológicos.

ARTICULO SEXTO. POLÍTICA QUE CONTEMPLA LICENCIAS, DESVINCULACIÓN, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS.

- El área contable 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 contable debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a en la Dirección de Sistemas.

- Todos los accesos y claves de usuario para el uso de los sistemas de información de la Cámara de Comercio de Ocaña deberán ser desactivados o cambiados después de que un funcionario cese de prestar sus servicios

- Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el documento de entrega de equipos tecnológicos (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

ARTICULO SEPTIMO. 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 vigilancia al acceso del personal a dichas áreas.

- La Cámara de Comercio de Ocaña deberá contar con los mecanismos de vigilancia y seguridad a los ambientes físicos donde se encuentren recursos informáticos, tales como sensores de humo, circuitos cerrados de televisión en los lugares que la empresa considere críticas.
- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios que pertenecen a la Dirección de Sistemas. 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.
- La Dirección de Sistemas debe registrar la entrada de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia.
- Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de La Cámara de Comercio sin previa autorización. Así mismo, ningún equipo de cómputo debe ser reubicado o trasladado de las instalaciones de la sede a la cual fue asignado. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

- Cualquier miembro de La Cámara de Comercio y/o tercero debe estar autorizado por la dirección de sistemas para ingresar con equipos donde puedan obtener información, estos pueden ser (video cámaras, celulares, cámaras fotográficas etc.).
- Las licencias deben ser custodiadas y controladas por el área de tecnología. Esta área debe realizar auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal y autorizado por el jefe de cada área.

ARTICULO OCTAVO. POLÍTICA PARA EL ACCESO Y SEGURIDAD DE LOS USUARIOS
Los usuarios de los recursos tecnológicos y los sistemas de información de la Cámara de Comercio de Ocaña realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual le es permitido el acceso.

- Todos los funcionarios que laboran deben tener acceso solo a la información necesaria para el desarrollo de sus actividades.
- Las claves de acceso de los sistemas de información de la entidad, no deben divulgarse hacia el exterior de la entidad, ni compartir sus cuentas de usuario y contraseñas con otros 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 la Dirección de Sistemas.
- La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.
- Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales. Este tamaño debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.
- Los funcionarios de la Cámara de Comercio de Ocaña son responsables de la información que manejan y deberán cumplir con los lineamientos generales y especiales dados por la Entidad y por la ley para protegerla, evitar pérdidas, accesos no autorizados, exposición y actualización indebida de la misma. Así mismo no deben suministrar información de la entidad a ningún ente externo sin las autorizaciones respectivas.
- Es deber del funcionario informarse acerca de los virus y como se difunden normalmente. Aprender las señales comunes de los virus, mensajes extraños que aparecen en la pantalla, rendimiento deficiente del sistema de datos perdidos e imposibilidad de tener acceso al disco duro. Se advierte algunos de estos problemas en el equipo, debe ejecutar inmediatamente el software de detención de virus para reducir las posibilidades de perder datos.
- Es responsabilidad del funcionario realizar la limpieza externa del equipo a su cargo.
- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la Cámara de Comercio de Ocaña deben hacerse responsables de las

acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

- Los funcionarios 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 Cámarade Comercio de Ocaña.
- Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.
- A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato la Dirección de Sistemas.
- Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.
- Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico de la Dirección de sistemas.
- Solamente los funcionarios de la Dirección de sistemas están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.
- Queda prohibido el uso de módems o conexión compartida en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación escrita por parte de Presidencia.
- La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios de sistemas autorizados por la Cámara de Comercio.
- La Cámara de Comercio ha suscrito con los fabricantes y proveedores un contrato de "LICENCIA DE USO" para los aplicativos que utiliza **(Windows, Office, Avast, Docuware, etc.)**. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Entidad.

ARTICULO NOVENO. 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 Ocaña será reglamentado por la Dirección de Sistemas, considerando las labores realizadas por los funcionarios y su necesidad de uso.

- Los funcionarios de la Cámara de Comercio de Ocaña no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Sistemas.
- Los funcionarios son responsables por la custodia de los medios de almacenamiento institucionales asignados.
- Los funcionarios no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la Cámara de Comercio de Ocaña.

ARTICULO DECIMO. POLITICAS DE ACCESO A REDES Y SUS RECURSOS.

La Dirección de Sistemas de la Cámara de Comercio de Ocaña, 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.

- La Dirección de Sistemas debe asegurar que las redes inalámbricas de la empresa cuenten con métodos de autenticación que eviten accesos no autorizados, dicha validación debe ser cambiada con una frecuencia no superior a los 3 meses.
- La Dirección de Sistemas debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de la Cámara de Comercio de Ocaña.
- 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.
- Se permite el acceso de dispositivos inteligentes a las redes inalámbricas de la Cámara de Comercio previa autorización y evaluación de las necesidades por parte de la Dirección de Sistemas.

ARTICULO UNDECIMO. POLÍTICA USO DEL CORREO ELECTRÓNICO

La Cámara de Comercio de Ocaña, 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.

- 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 Ocaña. 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 Ocaña 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 Ocaña y deben conservar en todos los casos el mensaje legal corporativo.

- Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.
- Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.
- En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente a la Dirección de Sistemas.

ARTICULO DECIMO SEGUNDO. POLITICAS DE USO ADECUADO DE INTERNET

La Cámara de Comercio de Ocaña 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.

- La Dirección de Sistemas 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.
- La Dirección de Sistemas 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 Ocaña 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 La Dirección de Sistemas, 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 Ocaña, de sus clientes y/o de sus funcionarios, con terceros.

- No utilizar canales de chat o grupos sociales como facebook, Messenger, etc., en horario laboral con fines personales sin previa autorización de la Cámara de Comercio de Ocaña.

ARTICULO DECIMO TERCERO. POLÍTICA SOBRE LA 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.

- 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 de la Jefatura de prensa y Comunicaciones de la Entidad.
- El jefe de Prensa y Comunicaciones de la Cámara de Comercio de Ocaña, será el responsable de la actualización de contenidos de las diversas secciones de la página. Dicha actualización se realizará simultáneamente al proceso de publicación, cuando sea necesaria o se presente alguna novedad.
- La Página Web de la Cámara de Comercio de Ocaña, 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 Ocaña, 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 Ocaña, así se reservan todos los derechos de propiedad intelectual sobre los contenidos de su autoría y sobre las que sean cedidas.
- La ejecución de actualizaciones en programación o desarrollo tendientes al mejoramiento de la página Web de la Cámara de Comercio de Ocaña, está delegado solamente a la Dirección de Sistemas.

ARTICULO DECIMO CUARTO. POLÍTICA PARA USO DE TERMINALES MÓVILES

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

- 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.
- La Dirección de Sistemas 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 Ocaña.
- La dirección de Sistemas debe implementar un método de bloqueo para los dispositivos móviles institucionales que serán entregados a los usuarios.
- La dirección de Sistemas y la Presidencia Ejecutiva son quienes autorizan la conexión de dispositivos móviles personales a la red institucional.

ARTICULO DECIMO QUINTO. POLITICA DE USO DE EQUIPOS PORTATILES Y DE ESCRITORIO

Los equipos de cómputo portátiles, se encuentran bajo la custodia de la Dirección de sistemas y están dispuestos para ser prestados a los funcionarios de la entidad ante cualquier situación que requiera la utilización de dicho equipo tecnológico; si la utilización del equipo de computo va a ser fuera de las instalaciones de la entidad se debe diligenciar documento que conste que se realizó la entrega de dicha herramienta y el funcionario que lo utilizará se hará responsable por este equipo mientras este en su poder.

- El antivirus siempre debe estar activo y actualizado
- No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de La Cámara de Comercio.
- Seguir las políticas de acceso remoto
- Cuando el equipo deba ser devuelto a La Cámara de Comercio para reparación, mantenimiento etc. La información confidencial deberá ser borrada y respectivamente guardada en una copia de respaldo.
- De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas.
- No dejar el computador portátil en lugares públicos.

- Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su mano.
- Cuando vaya en su carro este debe ir en el baúl.
- No prestar el computador portátil a familiares y/o amigos
- Los computadores de escritorio, computadores portátiles y demás recursos informáticos de la Cámara de Comercio de Ocaña, no deben ser utilizados para actividades personales o ajenas a la función asignada.
- Los computadores de escritorio, computadores portátiles y demás recursos informáticos de la Cámara de Comercio de Ocaña, deben ser operados y utilizados solamente por el personal que se encuentre autorizado para ello y/o el responsable de los mismos.
- Todos y cada uno de los computadores de escritorio, computadores portátiles y demás recursos informáticos asignados a una persona, son responsabilidad de la misma por el buen uso de los mismos. En caso de que el recurso informático vaya a ser utilizado por una persona diferente a la que se le asignó, este último debe asegurar y velar porque se haga buen uso de dicho recurso.
- Todos los computadores de escritorio, computadores portátiles y demás recursos informáticos deben ser apagados al finalizar la jornada laboral.
- La protección física de los computadores de escritorio, computadores portátiles y demás recursos informáticos, corresponde a las personas, a quienes se les asignaron, y es su deber notificar al departamento de sistemas sobre cualquier eventualidad que ocurra sobre dichos equipos.
- La dirección de sistemas es el único autorizado para realizar movimientos y asignaciones de recursos informáticos, por lo que está totalmente prohibida la disposición que de éstos pueda hacer cualquier usuario, aún si a este se le ha asignado el recurso.
- Los computadores de escritorio, computadores portátiles y demás recursos informáticos asignados a los usuarios de la Cámara de Comercio de Ocaña, deben someterse a todas las instrucciones, políticas y disposiciones que imparta el departamento de sistemas y que sean autorizadas por los niveles correspondientes.
- En caso de presentarse una falla o problema de hardware o software en un computador de escritorio, computador portátil y demás recursos informáticos de propiedad de la Cámara de Comercio de Ocaña, el usuario responsable del mismo deberá informarlo a la dirección de sistemas, para recibir soporte especializado.
- La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los computadores de escritorio, computadores portátiles y demás recursos informáticos propiedad de la Cámara de Comercio de Ocaña, solo puede ser realizado por los funcionarios autorizados por el departamento de sistemas. Por ningún motivo los usuarios podrán abrir o desarmar los equipos de cómputo.
- Los computadores de escritorio, computadores portátiles y demás recursos informáticos propiedad de la Cámara de Comercio de Ocaña que se encuentren por fuera de las instalaciones, deben ser custodiados de manera adecuada por sus responsables, evitando ser desatendidos en lugares públicos.

- En caso de pérdida, robo o extravío de computadores de escritorio, computadores portátiles y/o demás recursos informáticos propiedad de la Cámara de Comercio de Ocaña, se deberá informar directamente por escrito a la presidencia ejecutiva.
- Cuando un usuario inicie o termine su vinculación laboral con La Cámara de Comercio de Ocaña o por alguna otra circunstancia deje de utilizar el computador de escritorio, computador portátil o el recurso informático asignado, deberá entregar dicho recurso formalmente a la dirección de sistemas.
- Está prohibido el ingreso a las instalaciones de La Cámara de Comercio de Ocaña, de recursos informáticos que no sean propiedad de la entidad, salvo aquellos que estén relacionados en los acuerdos de conexión a la red por parte de terceros y sean usados para cumplir el objeto de algún contrato vigente entre el tercero y la Cámara de Comercio de Ocaña. Por ningún motivo se permite el ingreso a las instalaciones de la Cámara de Comercio de Ocaña, de recursos informáticos que sean propiedad de los empleados.
- Sólo se permite conectar a la red corporativa aquellos recursos informáticos que estén autorizados, por ser propiedad de la Cámara de Comercio de Ocaña, o por estar relacionados en algún acuerdo de conexión a la red por parte de terceros.
- Todo funcionario solo podrá tener asignado para sus labores un computador de escritorio ó un computador portátil, no podrá tener para su disposición permanente el uso de dos recursos informáticos. La decisión del tipo de recurso que deberá utilizar es tomada en
- conjunto con la Presidencia Ejecutiva, el Director de departamento y la Dirección de sistemas.
- No se debe interrumpir las instalaciones, actualizaciones o parches de seguridad que se envíen de manera remota a los computadores de escritorio, computadores portátiles y demás recursos informáticos.

ARTICULO DECIMO SEXTO. POLITICAS PARA CONEXIONES REMOTAS

La Cámara de Comercio de Ocaña 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.

- 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 Ocaña y deben acatar las condiciones de uso establecidas para dichas conexiones.
- La dirección de sistemas debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la Cámara de Comercio de Ocaña.
- Al realizar una conexión remota a la plataforma tecnológica de la Cámara de Comercio de Ocaña, se mantener por parte de la dirección de sistemas constante monitoreo de las actividades que se estén realizando.

ARTICULO DECIMO SEPTIMO. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO.

La Cámara de Comercio de Ocaña 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.

- La dirección de sistemas 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 Ocaña y los servicios que se ejecutan en la misma.
- La dirección de sistemas 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.
- La dirección de sistemas 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.
- La dirección de sistemas, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- La dirección de sistemas, 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 la dirección de sistemas; 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 a la dirección de sistemas tome para tomar medidas de control pertinentes.

ARTICULO DECIMO OCTAVO. POLITICAS DE COPIAS DE SEGURIDAD

La Cámara de Comercio de Ocaña 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 La dirección de sistemas, 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.

- La dirección de sistemas, 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.
- La dirección de sistemas 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.
- La dirección de sistemas, 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.
- La dirección de sistemas 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 Ocaña identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

ARTICULO DECIMO NOVENO. 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.

- La Dirección de sistemas y el área de Control interno deben realizar un plan de contingencia para la continuidad de negocio dentro de la Cámara de Comercio de Ocaña.

CAPITULO IV
SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ARTICULO VIGESIMO.
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 Ocaña.

Con el objetivo de aplicar medidas correctivas conforme a la gravedad del desacato y mitigar posibles afectaciones contra la seguridad de la información, Las estas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo a las circunstancias.

CAPITULO V
ACTUALIZACIÓN, MANTENIMIENTO Y DIVULGACIONDE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

ARTICULO VIGESIMO PRIMERO.
Éste documento se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

La presidencia o la persona designada por la presidencia, debe aprobar el documento, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes.

El mecanismo de notificación y divulgación de los cambios realizados a estas políticas será mediante correo electrónico.

PUBLIQUESE Y CUMPLASE;

RUBEN DARIO ALVAREZ
Presidente Ejecutivo