EL TIEMPO CASA EDITORIAL	SISTEMA NORMATIVO DOCUMENTO DE POLÍTICA					
Nombre Política:	Tratamiento información confidencial					
Elaborado por:	Gerencia de Tecnología y Gerencia Legal					
Aprobado por:	Vicepresidente Ejecutivo y Gerencia General Financiera y USC					
Ámbito aplicación:	CEETTV, CEET y subsidiarias (en adelante mencionadas como CEET)					
Destinatarios:	Todos los colaboradores					
Clasificación Doc.:	Uso interno ☑ Confidencial ☐					
Rango: **B** **Fechas:**	**Emisión:**	01/12/2016	**Actualización:**	01/12/2016	**Codificación:**	PO118-01

POLITICA TRATAMIENTO INFORMACIÓN CONFIDENCIAL

1.- Objetivo.

Esta norma regula el tratamiento de la información confidencial dentro de CEET, es de estricto cumplimiento tanto para empleados en nómina como para los contratistas o empleados temporales que mantengan una relación mercantil con la misma.

Se considera información confidencial toda aquella información de carácter mercantil que pude incluir, entre otros, planes de negocio y de desarrollo, información técnica, financiera y legal, planes de productos y servicios, información de precios, informes de mercadeo, análisis y proyecciones, especificaciones, diseños, software, datos, secretos industriales, know how y otras informaciones de negocios o técnicas, información personal de los empleados que pueda afectar su privacidad, políticas identificadas expresamente con confidenciales, informes y actas emitidas por las áreas corporativas.etc.

2.- Clasificación de activos y responsabilidades.

Todos los activos de información pertenecientes a las sociedades a las que afecta esta política deberán ser identificados, clasificados y valorados según su grado de sensibilidad y criticidad e impacto para la organización, con el fin de determinar los niveles de protección adecuados. Así mismo, cada activo deberá establecer claramente los usuarios, dueños y custodios durante el ciclo de vida de los mismos.

Se establecen en CEET las siguientes clasificaciones:

- **Uso externo:** todos aquellos documentos que se usan para información con el exterior de la compañía; clientes, proveedores, socios de negocio, etc. y cuya información sea de uso público y que no represente un riesgo para la inhabilitación de negocios de CEET o el deterioro de su imagen.
- **Uso interno**: todos aquellos documentos que se usan para la operación interna de procesos y negocios.
- **Uso restringido o Confidencial**: documentos con uso restringido en cuanto a su contenido al interior de la compañía y cuya revelación pone en riesgo a los negocios de CEET, podría dañar su imagen y causar una pérdida de valor.

La responsabilidad de establecer la adecuada clasificación y dotar a la organización de las medidas de seguridad, se determinará en función del rol de cada usuario, que puede categorizarse en alguno de los siguientes grupos:

- **Custodios de los datos**: son aquellos responsables de implementar los requerimientos de seguridad y las reglas de negocio en los sistemas de TI para garantizar el seguro transporte, almacenamiento y disponibilidad de la información. Deben además acatar y cumplir los requerimientos de seguridad sobre la información y el buen uso de los sistemas de TI.

- **Dueño de la información:** Son los responsables de clasificar la información, pues son ellos quienes conocen el valor de la misma, además son responsables de garantizar que existan los controles apropiados para abordar la integridad, confidencialidad y disponibilidad a implementarse en los sistemas de TI. También son responsables de los cambios registrados en los sistemas de TI y autorizan o deniegan el acceso a la información. Deben además acatar y cumplir los requerimientos de seguridad sobre la información y el buen uso de los sistemas de TI.

- **Usuarios de la información:** son aquellos que utilizan la información y los sistemas de TI creándola, modificándola o eliminándola siguiendo unas reglas de negocio establecidas; deben además acatar y cumplir los requerimientos de seguridad sobre la información y el buen uso de los sistemas de TI.

3.- Reglas generales.

Aquellos que se encuentren definidos en el alcance de esta política, deberán guardar la máxima reserva y no divulgar ni utilizar pública y/o directamente, ni a través de terceras personas o empresas, la información declarada como confidencial, (en formato físico o electrónico), a la que tengan acceso durante su relación laboral o colaboración mercantil con la empresa y/o empresas pertenecientes a las sociedades de CEET, para fines diferentes a los definidos en los contratos, acuerdos o relaciones mercantiles establecidas y con la que se puedan beneficiar o causar un daño a CEET por la revelación de la misma. Esta obligación continuará vigente tras la extinción del contrato laboral o la relación mercantil.

No se podrá enviar, sin la debida autorización, información confidencial de la empresa al exterior o a destinatarios no autorizados, mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.

En el caso de que, por motivos directamente relacionados con el puesto de trabajo o la colaboración mercantil, el empleado o colaborador entre en posesión de información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le de derecho alguno de posesión, o titularidad o copia sobre la referida información.

Asimismo, deberá devolver dichos materiales a la empresa, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral o mercantil. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de la empresa, no supondrá, en ningún caso, una modificación de esta disposición.

Sólo las personas autorizadas directamente por el área de Asuntos Corporativos podrán atender a encuestadores y complementar cuestionarios en los que se solicite cualquier tipo de información de datos relativa a la empresa, a excepción de aquellos casos en que ya esté establecido un acuerdo con la entidad para el reporte de la información por parte de las distintas áreas de CEET y que se encuentren en conocimiento de Asuntos Corporativos.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos y una violación a las obligaciones de confidencialidad que puede acarrear las consecuencias penas de prisión y pago de indemnizaciones por daños y perjuicios.

4.- Acuerdos de confidencialidad

Para CEET es de gran importancia la confidencialidad de la información que se produce, adquiere o se le entrega a la organización. La dinámica de la organización exige que la información sea manipulada por empleados, compartida o trasmitida a terceros.

Por esta razón y para garantizar la confidencialidad se hace necesario que se manejen dentro de los contratos con empleados, temporales, contratistas, consultores internos o externos y proveedores de servicios, acuerdos de confidencialidad para tener garantías jurídicas sobre la información que se maneja o comparte y que participen en procesos, negocios o proyectos de carácter confidencial; este acuerdo debe ser aceptado y entendido por las partes.

Es responsabilidad del Área Jurídica y de Recursos Humanos mantener y exigir este acuerdo de confidencialidad con cualquiera que desee realizar negocios o tener una relación laboral con CEET. Así mismo es responsabilidad del líder del proyecto, o dueño de la información realizar la solicitud a RRHH, o quien tuviere esta responsabilidad, para que este requerimiento sea cumplido.

A nivel general, será obligatorio la firma de acuerdos de confidencialidad en los siguientes casos:

- Todo el personal vinculado a las áreas de USC.
- Auditoría Interna y Jurídico.
- Gerentes, Directores y Jefes de todas las áreas.
- Otros cargos que por sus funciones y a juicio del gerente de la UEN o de RRHH sea requerido expresamente.
- Personal vinculado a proyectos.

5.- Recomendaciones de uso.

Con el fin de mantener la debida confidencialidad de la información a la que se tiene acceso desde el computador personal u otros sistemas de información, los usuarios en general deben:

- Etiquetar adecuadamente la información para poner en conocimiento de otros el tipo de clasificación al que se refiere un activo de información.
- Mantener la reserva de los usuarios y contraseñas que identifican y autorizan el acceso a la información.
- Cambiar las contraseñas periódicamente.
- Los filtros de pantalla con contraseña se deben activar manual y/o automáticamente cuando el usuario se ausenta de su puesto de trabajo.
- Mantener en lugar seguro y protegido los sistemas externos de almacenamiento de información.
- Cumplimiento de las especificaciones en la política sobre tratamiento de archivos y documentos no automatizados.
- Queda prohibida la instalación, en los computadores o Laptops personales de la empresa, de programas que permitan monitorear de forma no autorizada la actividad del usuario y enviar al exterior de la empresa información confidencial.

Para mayor información, consultar la política relativa a la utilización de los sistemas de información.