


	SECAP LTDA.	Página	1 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

1. OBJETIVO
2. ALCANCE
3. RESPONSABLE
4. DEFINICIÓN DE TÉRMINOS
5. DESARROLLO
6. ANEXOS
7. CONTROL DE CAMBIOS

ELABORO	REVISÓ	APROBÓ
 LAURA KATERINE LAMPREA MARTÍNEZ Oficial de Cumplimiento	 ROBERTO MOLINA CASTAÑO Director Nacional de Operaciones y Seguridad	 MARÍA MARCELA MARTÍNEZ CASTAÑEDA Gerente General

	<h1>SECAP LTDA.</h1>	Página	2 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

1. OBJETIVO

La Política Integral de Seguridad de la Información y Protección de datos Personales en Secap Ltda., busca evitar que las amenazas latentes en el entorno, personal activo y/o retirado que puedan acceder, sustraer, manipular, suministrar y/o entregar en forma indebida o deteriorar la información producida para los procesos de la compañía y en el resultado de los procesos disminuir la posible pérdida de información.

2. ALCANCE

Esta política es aplicable a todas las áreas involucradas en la operación de **Secap Ltda.**

3. RESPONSABLES

- ✓ Gerente General.
- ✓ Director Nacional de Operaciones y Seguridad.
- ✓ Auxiliar de sistemas
- ✓ Todo el Personal involucrado en el manejo, manipulación, acceso de información y a los sistemas.

4. DEFINICIONES

- ✓ **INFORMACIÓN:** Son datos o conjunto de datos (sonidos, imágenes, alfanumérico, gráficos, textos), convertidos a un lenguaje significativo y útil para usuarios finales y específicos.
- ✓ **DOCUMENTO:** Es cualquier medio de registro o soporte del conocimiento susceptible de ser descrito y analizado, para posterior recuperación.
- ✓ **MANIPULACIÓN:** Uso correcto o incorrecto de los sistemas de información (equipos de cómputo), y de la información (Registro), para fines determinados o indeterminados.
- ✓ **DERECHOS DE AUTOR:** La invención, mejora, implementación y creación realizada por el trabajador dentro de las instalaciones y con los elementos de la empresa pertenece al empleador y su manipulación indebida tendrá efectos jurídicos y penales.
- ✓ **ACUERDO DE CONFIDENCIALIDAD:** Es una condición pactada bien sea por escrito que se fija en una relación comercial o laboral con el propósito que las partes contratantes mantengan en secreto o reserva aspectos propios que sólo se podrán conocer con ocasión a la relación que se presenta. Este Acuerdo de Confidencialidad se da con frecuencia en aquellas labores donde el Trabajador o el Contratista manejan aspectos propios a mantener en reserva de la empresa como investigaciones científicas, industriales o comerciales, futuros lanzamientos

	<h1>SECAP LTDA.</h1>	Página	3 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

de productos, académicas o por seguridad como es la información de movimientos bancarios y de los procesos que conoce un funcionario de una empresa o de un cliente, etc.

- ✓ **BACK-UP:** Copia de seguridad de uno o más archivos informáticos, que se hace, generalmente para prevenir posibles pérdidas de información.

5. PROCEDIMIENTO

5.1 ACCESO A LA INFORMACIÓN

No deberá existir sobre el escritorio información confidencial o de importancia para la organización a la vista de cualquier persona, ni referencias sobre los códigos de acceso de la persona encargada de algún cargo que sea parte de la organización.

Se restringe el acceso a archivos Administrativos, archivo Operativo, Tesorería y Nómina, al personal No Autorizado con el fin de salvaguardar la información que allí se almacena.

Cuando las personas con permisos se encuentren en las respectivas dependencias de la compañía, estarán en todo momento, acompañadas del personal de Secap Ltda.

La Gerencia General y de Operaciones restringe el acceso a las bases de datos en las que se almacena la información empresarial, para asegurar su correcta utilización.

Para dar cumplimiento a esta política, la compañía diseña protocolos y procedimientos que regulan la administración de la información.

5.2 SEGURIDAD DE LA TECNOLOGÍA DE INFORMÁTICA

Para la compañía es vital Proteger la información, enviada y recibida por medio físico o electrónico.

Por este motivo el personal que tiene computador, debe proteger el ingreso al sistema con una clave personalizada, que será de uso restringido y personal.

La clave de acceso para ingresar al sistema debe expirar cada 30 días notificando al usuario para su cambio obligatorio.

La Clave de usuario para ingreso al sistema de trabajo, debe contener un mínimo de 8 caracteres.

Es responsabilidad de los usuarios del correo electrónico y del ingreso a internet, el uso con responsabilidad y criterio de estas herramientas, al no permitir el acceso a páginas y comunicados diferentes a los necesarios para el desempeño de su labor.

 SECAP <small>TALENTO HUMANO CON SEGURIDAD</small>	<h1 style="text-align: center;">SECAP LTDA.</h1>	Página	4 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

Cuando los funcionarios se ausenten por un largo periodo de su puesto de trabajo, deberán dejar su equipo con clave de reanudación.

Al término de la jornada laboral, los funcionarios deben dejar la documentación dentro de los escritorios y/o archivadores bajo llave.

Se deberá guardar copia de los medios magnéticos en un disco externo el cual deberá estar en custodia fuera de las instalaciones de la sede Bogotá y será responsabilidad directa e intransferible de la Gerencia General y/o Gerencia de Operaciones y Seguridad.

5.3 USO DE CONTRASEÑAS

Todos los funcionarios que deban tener acceso a las herramientas (equipos de cómputo), que apoyan el sistema de información, cuentan con clave de acceso y tiene definidos perfiles de usuarios que aseguren la autorización para grabar, modificar y consultar información.

Las claves asignadas para acceder a los sistemas de información son de uso personal e intransferible y está bajo la responsabilidad de cada usuario.

Los funcionarios deben cambiar la clave cada treinta días o cuando lo considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

Cuando el funcionario deja el puesto de trabajo, se deben cerrar las aplicaciones que se estén utilizando.

Los archivos administrativos que se utilizan en procesos empresariales o equipos de cómputo requieren una clave o contraseña especial, esta debe ser notificada a la Gerencia de General y de Operaciones.

5.4 PROTECCIÓN DE LA INFORMACIÓN

El Auxiliar de sistemas y las Coordinadoras de Operaciones a nivel nacional deberán realizar un Back up, de los procesos realizados mensualmente en medio magnético (CD, DVD). Este back up será entregado al Gerente de operaciones y seguridad o auxiliar de sistemas, el cual consignará la información en el disco duro interno y externo.

Los documentos y registro e información correspondiente al proceso se encuentran almacenados en dos (2) discos duros uno externo y otro Interno, esto con el fin de tener un respaldo en caso de pérdida o daño que afecte la información, el disco duro interno se encuentran a Cargo del Gerente de operaciones y el Auxiliar de Sistemas quienes son las personas autorizadas para tener acceso de manera permanente a esta información.

	<h1>SECAP LTDA.</h1>	Página	5 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

5.5 HARDWARE Y SOFTWARE

No se pueden ingresar a la empresa Secap Ltda., hardware ni software personales sin previa autorización del proceso de Gestión de Sistemas Informáticos.

No se deben bajar ni actualizar programas desde Internet en los equipos de la empresa, salvo las actualizaciones autorizadas por la Gerencia de Operaciones y Seguridad.

La instalación de software que desde el punto de vista de la Gerencia General y de Operaciones pudiera poner en riesgo los recursos de la institución no está permitida.

5.6 VIRUS

Los Usuarios de cada uno de los Sistemas de información son responsables de solicitar soporte informático en caso de encontrar situaciones sospechosas en el sistema.

No instalar "vacunas" sin la autorización de la Gerencia de Operaciones y Seguridad o el Auxiliar de Sistemas, Estas aunque parezca paradójico, pueden estar infectadas.

5.7 ACCIONES DISCIPLINARIAS

Se debe firmar por parte de cada funcionario que posee equipos de cómputo y que manipule información la Política Integral de Seguridad de la Información y la Cláusula de Confidencialidad, con la cual se tomaran medidas disciplinarias desde el llamado de atención, la suspensión del trabajador, las acciones legales y penales a que haya lugar, en caso de ser identificado el abuso de de los sistemas de computación, tecnología de informática, detectar el acceso inapropiado, sustraer, manipular, suministrar, alterar y/o entregar en forma indebida o deteriorar la información producida para los procesos de la compañía, datos comerciales y del negocio, así como el resultado de los mismos por parte del personal activo y/o retirado

5.8 CLAUSULA MANEJO Y ABUSO DE LOS SISTEMAS DE COMPUTACIÓN Y TECNOLOGÍA DE LA INFORMACIÓN

El personal de Secap Ltda., se compromete a:

- Los Usuarios de cada uno de los Sistemas de información (equipos de cómputo), son responsables de no acceder a páginas y programas que no se encuentren autorizados por la Gerencia General y de Operaciones.
- No se podrá acceder desde los equipos de cómputo a páginas que contengan información que atenten contra la moral de las personas y de la compañía, páginas

	<h1>SECAP LTDA.</h1>	Página	6 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

de redes sociales, páginas de chateo, páginas para observar y grabar de videos, páginas para desarrollar juegos.

- Con el fin de identificar el abuso de los sistemas de computación y de tecnología de informática y detectar el acceso inapropiado y la manipulación indebida o alteración de los datos comerciales y del negocio, se colocara en los equipos de cómputo un sistema que permitirá observar la utilización de los mismos.

5.9 EFECTOS QUE TIENE DIVULGAR O UTILIZAR INDEBIDAMENTE LA INFORMACIÓN Y/O ASPECTOS RESERVADOS DE LA COMPAÑÍA

La esencia de los Acuerdos de Confidencialidad es imponer sanciones a quien incumple con la obligación de mantener en reserva aspectos propios de la actividad de los contratantes.

Por violar dicha Confidencialidad, es Justa Causa para dar por terminado el Contrato de Trabajo (artículo 62 numeral. 8º Código sustantivo del trabajo) y no da derecho al reconocimiento de Indemnización al trabajador.

Asimismo, al ser una [Obligación Especial del Trabajador](#), según el artículo 58 numeral 2º que reza: “No comunicar con terceros, salvo la autorización expresa, las informaciones que tenga sobre su trabajo, especialmente sobre las cosas que sean de naturaleza reservada o cuya divulgación pueda ocasionar perjuicios al empleador, lo que no obsta para denunciar delitos comunes o violaciones del contrato o de las normas legales del trabajo ante las autoridades competentes”

Así mismo se podría incurrir en un delito. El Código Penal establece varios Tipos Penales (delitos) relacionados con la violación a la Confidencialidad o Reserva, veamos:

- | | | |
|---|--------------|---|
| ✓ | Artículo 194 | Divulgación y Empleo De Documentos Reservados. |
| ✓ | Artículo 308 | Violación de Reserva Industrial o Comercial. |
| ✓ | Artículo 418 | Revelación de Secreto. |
| ✓ | Artículo 419 | Utilización de Asunto Sometido a Secreto o Reserva. |
| ✓ | Artículo 420 | Utilización Indebida de Información Oficial Privilegiada. |
| ✓ | Artículo 463 | Espionaje. |

6. PLAN DE CONTINGENCIA DE LA INFORMACIÓN

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, para establecer medidas destinadas a salvaguardar la

	SECAP LTDA.	Página	7 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

información contra los daños producidos por hechos naturales o por el hombre. La información como uno de los activos más importantes de la Organización, es el fundamento más importante de este Plan de Contingencia.

6.1 CONTROL DE DOCUMENTOS EN TRANSITO

Los documentos en tránsito serán controlados por la Asistente Administrativa de Operaciones, quien custodia el archivo general de la compañía, el cual se encuentra bajo llave, este archivo se encuentra clasificado por clientes y en el reposan los documentos físicos de cada candidato.

6.2 MANIPULACIÓN DE DOCUMENTOS

El proceso operativo de la compañía se desarrolla con el principio de compartimentación, esto con la finalidad de evitar filtración, alteración, modificación o pérdida de la información y documentación física. Por este motivo la información es diseminada suministrando la documentación e información necesaria para desarrollar las diferentes etapas del proceso.

6.3 TRAZABILIDAD DE LOS DOCUMENTOS EN TRANSITO

La documentación extraída del archivo general entregada a los empleados de la compañía para su consulta quedara registrada, en este registro se encuentra relacionado el nombre de la persona que solicita el documento, el nombre del candidato y la firma de quien recibe el documento, quien solicita la documentación se encuentra autorizada para tener custodia del documento por un día laboral bajo los parámetros de seguridad establecidos por la compañía en sus políticas y procedimientos, esta persona será responsable de la documentación y el plazo máximo de entrega del documento es al término de la jornada laboral.

Una vez terminada la Jornada Laboral todos y cada uno de los documentos no podrá reposar en ningún lugar diferente al Archivo General bajo llave.

La llave del Archivo General será custodiada en cofre de llaves, el cual se encuentra en la Oficina Administrativa.

6.4 CONFIDENCIALIDAD

Todas las personas que intervengan en el tratamiento de datos personales dentro y fuera de la compañía están obligadas a garantizar la reserva de la información inclusive después de finalizar su relación con alguna de las labores que comprenda el tratamiento.

	<p>SECAP LTDA.</p>	Página	8 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

El personal de la compañía es sensibilizado con capacitaciones de Seguridad de la Información y Políticas Internas de la compañía en control de documentos, creando una Cultura de Seguridad. Adicional a esto las personas que laboran en el Secap Ltda., pasan por un estudio de seguridad previo a su vinculación y dentro de su duración en la compañía se realizan estudios de actualización cada dos años.

6.5 ARCHIVO PERMANENTE

La custodia permanente de la información se realiza en medio magnético, por este motivo los documentos susceptibles de custodia permanente son escaneados y archivados en un Disco Duro Externo con protección y bajo la custodia del Gerente Nacional De Operaciones y Seguridad, el documento físico que no es entregado a un tercero se tritura e incinera cada 30 días, actividad que debe ser registrada mediante acta del respectivo procedimiento y firmado por el personal de las diferentes áreas del proceso.

6.6 CUSTODIA TEMPORAL DE LA INFORMACIÓN

La documentación suministrada por el candidato es entregada a la Compañía Secap Ltda., compañía autorizada por el titular de la información en el momento de la realización de la Visita Domiciliaria. El tiempo que Secap Ltda., tenga en su custodia esta información será protegida bajo condiciones y parámetros específicos de Seguridad contemplados en el Manual de Seguridad, procesos como la administración del riesgo, control de documentos y registros etc.

	<p>SECAP LTDA.</p>	Página	9 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

7. ANEXOS

ACUERDO DE CONFIDENCIALIDAD A EMPLEADOS

Entre los suscritos a saber, por una parte **MARIA MARCELA MARTINEZ CASTAÑEDA**, mayor de edad y domiciliada en la ciudad de **BOGOTA**, identificada como aparece al pie de su respectiva firma, y obrando en representación legal de **Secap Ltda.**, y por la otra, _____, mayor de edad y domiciliado en la ciudad de _____, identificado(a) como aparece al pie de su firma, se ha acordado celebrar el presente Acuerdo de Confidencialidad que se regirá por las siguientes cláusulas, previas las siguientes **CONSIDERACIONES**.

- Las partes están interesadas en el servicio de _____
- Debido a la naturaleza del trabajo, se hace necesario que se maneje y conozca información confidencial y/o información sujeta a derechos de propiedad intelectual, antes, durante y en la etapa posterior.

CLÁUSULAS

PRIMERA – OBJETO. El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre ellas, incluyendo información objeto de derecho de autor, patentes, técnicas, modelos, invenciones, know-

	<h1>SECAP LTDA.</h1>	Página	10 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

how, procesos, algoritmos, programas, ejecutables, investigaciones, detalles de diseño, información financiera, lista de clientes, inversionistas, empleados, relaciones de negocios y contractuales, pronósticos de negocios, planes de mercadeo e cualquier información revelada sobre terceras personas.

SEGUNDA – CONFIDENCIALIDAD. Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata. Se considera también información confidencial: a) Aquella que como conjunto o por la configuración o estructuración exacta de sus componentes, no sea generalmente conocida entre los expertos en los campos correspondientes. b) La que no sea de fácil acceso, y c) Aquella información que no esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial.

TERCERA – EXCEPCIONES. No habrá deber alguno de confidencialidad en los siguientes casos: a) Cuando la parte receptora tenga evidencia de que conoce previamente la información recibida; b) Cuando la información recibida sea de dominio público y, c) Cuando la información deje de ser confidencial por ser revelada por el propietario.

CUARTA – DURACION. Este acuerdo regirá durante el tiempo que dure la labor desempeñada como funcionario activo y hasta un término de diez años contados a partir de su fecha de su desvinculación de la empresa.

QUINTA – DERECHOS DE PROPIEDAD. Toda información intercambiada es de propiedad exclusiva de Secap Ltda., En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso o de terceros.

SEXTA – ASPECTO LEGAL. La esencia de los Acuerdos de Confidencialidad es imponer sanciones a quien incumple con la obligación de mantener en reserva aspectos propios de la actividad de los contratantes.

Por violar dicha Confidencialidad, es Justa Causa para dar por terminado el Contrato de Trabajo (artículo 62 numeral. 8º Código Laboral) y no da derecho al reconocimiento de Indemnización al trabajador.

Asimismo, al ser una [Obligación Especial del Trabajador](#), según el artículo 58 numeral 2º que reza: “No comunicar con terceros, salvo la autorización expresa, las informaciones que tenga sobre su trabajo, especialmente sobre las cosas que sean de naturaleza reservada o cuya divulgación pueda ocasionar perjuicios al empleador, lo que no obsta para denunciar delitos comunes o violaciones del contrato o de las normas legales del trabajo ante las autoridades competentes”

Así mismo se podría incurrir en un delito. El Código Penal establece varios Tipos Penales (delitos) relacionados con la violación a la Confidencialidad o Reserva, veamos:

	<h1>SECAP LTDA.</h1>	Página	11 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

SEPTIMA – MODIFICACIÓN O TERMINACIÓN. Este acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de ambas partes.

Nombre y Apellido

Cedula de Ciudadanía.

Firma Funcionario.

CLAUSULA MANEJO Y ABUSO DE LOS SISTEMAS DE COMPUTACIÓN Y TECNOLOGÍA DE LA INFORMACIÓN

Yo, _____, identificado con la Cédula de Ciudadanía Número _____ de _____ del proceso de _____, recibo _____, confirmo que se encuentra en buen estado, también que realizó el respectivo Backup de la información, y afirmo que tengo conocimiento de la Política de Seguridad de Información sustentada en que:

- Los Usuarios de cada uno de los Sistemas de información (equipos de cómputo), son responsables de no acceder a páginas y programas que no se encuentren autorizados por la Gerencia General y de Operaciones.
- El equipo deberá cuidarse y quedara como responsable en caso de daño o pérdida, por lo que cada cambio de puesto o de equipo debe ser informado al área de sistemas, o al supervisor encargado.
- No se podrá acceder desde los equipos de cómputo a páginas que contengan información que atenten contra la moral de las personas y de la compañía tales como: redes sociales, chat, Canales de videos, juegos, reservaciones y páginas para adultos.
- Por ultimo con el fin de identificar el abuso de los sistemas de computación, tecnología, acceso inapropiado, manipulación indebida, alteración de los datos comerciales y del negocio, se dispondrá en los equipos de cómputo la personalización de la contraseña según lo programado en el sistema, además la navegación y telefonía será monitoreado detalladamente desde los servidores

	SECAP LTDA.	Página	12 de 12
		Versión	5
		Fecha de Aprobación	31/10/2012
		Fecha Última Actualización	10/08/2015
CÓDIGO: PR-05-13	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

Firewall y Asterisk con los que cuenta la compañía, cualquier anomalía o falta que se detecte, será informada a su jefe inmediato.

Nombre y Apellido

Fecha

Cedula de Ciudadanía.

Firma Funcionario.