
	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX


Política de Seguridad Informática

	SERVAGRO LTDA	Fecha.	19 Enero 2015
		Versión.	1.2.5
	Sección: Seguridad y Control	Cód.	XXXXX

1	Contenido	Pág.
2	EXPOSICIÓN DE MOTIVOS	4
2.1	Verificación y revisión de la red	4
3	RESUMEN	5
3.1	Definición	5
4	INTRODUCCIÓN	6
5	POLÍTICAS DE SEGURIDAD.....	7
5.1	Equipos de cómputo.....	7
5.1.1	De la instalación del equipos de cómputo	7
5.1.2	Del mantenimiento del Equipo de Computo	7
5.1.3	De la actualización del equipo de cómputo	8
5.1.4	De la reubicación del equipo de cómputo.....	8
5.2	Control de accesos.....	8
5.2.1	Del acceso a Áreas Críticas	8
5.2.2	Del control de acceso al equipo de computo	9
5.2.3	Del control de acceso local de la red.....	9
5.2.4	Del control de acceso remoto	9
5.2.5	Del acceso a los sistemas administrativos	10
5.2.6	De las WWW	10
5.3	Utilización de los recursos de la red	11
5.4	Del software.....	11
5.4.1	De la adquisición del software	11
5.4.2	De la instalación del software	11
5.4.3	De la actualización del software.....	12
5.4.4	De la auditoria del software instalado.....	12
5.4.5	Del software de propiedad de la empresa	12
5.4.6	De la propiedad intelectual.....	13
5.5	Supervisión y evaluación	13
5.6	Copias de seguridad y Backups.....	13
6	GENERALES.....	14

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

7	SANCIONES	15
8	RECOMENDACIONES.....	16
9	PLAN DE CONTINGENCIA INFORMÁTICO	17
9.1	Introducción	17
9.2	Objetivos	17
9.3	Identificación de procesos y servicios	18
9.3.1	Principales Procesos de Software Identificados.....	18
9.3.2	Principales servicios que deberán ser restablecidos Y/O recuperados.....	18
9.4	Minimización del riesgo	18
9.4.1	Incendio o Fuego	19
9.4.2	Robo Común de Equipos y Archivos.....	19
9.4.3	Falla en los Equipos	20
9.4.4	Fenómenos Naturales.....	21

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

2 EXPOSICIÓN DE MOTIVOS

Ante el esquema de globalización que las tecnologías de la información se han originado principalmente por el uso masivo y universal de la internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc. Es decir en transgresores.

Conforme que las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

En nuestro país no existe una sola institución que no se haya visto sujeta a los ataques en sus estructura de red, tanto desde el interior como el exterior, basta decir que cuando estamos en la internet o haber encendido el equipo de computo estamos sujetos a un ataque pero hay gente que se involucran y están pendientes de este tipo de delito informático, tratando de contrarrestar y anular estas amenazas reales.

2.1 Verificación y revisión de la red


Después del diagnostico que se llevo a cabo, se observo la carencia de un inventario detallado de los equipos de computo de toda la empresa y sus sucursales, que se encuentran en la carpeta Cód. INVSLTDA001, lo cual se hace difícil su administración.

Nuestra carencia de recursos humanos involucrados en seguridad, la escasa concientización a los usuarios, la falla de visión y las limitantes económicos ha retrasado el plan de seguridad informática que se requiere.

El objetivo principal de la oficina de SISTEMAS es brindar a los usuarios los recursos informáticos con cantidad y calidad que demandan, esto es, que tengamos continuidad en el servicio los 365 días del año confiable. Así, la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta Servagro Ltda. Son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

La seguridad de las instituciones en muchos de los países se ha convertido en cuestión de seguridad nacional, por ello contar con un documento de Política de Seguridad Informática es imprescindible y debe de plasmar mecanismos confiables que con base en la política institucional proteja los activos de la empresa.

Así que ante este panorama surge el siguiente proyecto de políticas rectoras que harán que la oficina de SISTEMAS pueda disponer y solicitar de los ejes de proyección que en materia de seguridad informática la empresa requiera.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX


3 RESUMEN

El presente es una propuesta de las Políticas de Seguridad que en materia de informática y de comunicaciones digitales de la oficina de SISTEMAS de SERVAGRO LTDA, ha elaborado, para normar a la empresa.

Algunas acciones que por la naturaleza extraordinaria tuvieron que ser llevadas a la práctica como son: los inventarios, verificaciones de la red, su control en el internet y mecanismos en firewall, se mencionan, así como todos los aspectos que representan un riesgo o las acciones donde se ve involucrada y que compete a las tecnologías de la información; se han contemplado también las políticas que reflejan la visión de la actual administración respecto a la problemática de seguridad informática empresarial.

3.1 Definición

La propuesta ha sido detenidamente paneada, analizada y revisada a fin de no contravenir con las garantías básicas del individuo y no pretender ser una camisa de fuerza y más bien muestra una buena forma de operar el sistema con seguridad, respetando en todo momento estatutos y reglamentos vigentes de la empresa.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX


4 INTRODUCCIÓN

Los requerimientos de seguridad que involucran las tecnologías de la información en pocos años han cobrado un gran auge, y más aún con las de carácter globalizador como son la de internet y en particular la relacionada con la WEB, la visión de nuevos horizontes explorando más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales desarrollen políticas que norman el uso adecuado de estas destrezas de la tecnología y recomendaciones para aprovechar estas ventajas, y evitar su uso indebido, ocasionando problemas en los bienes y servicios de las empresas.

De esta manera, las Políticas de Seguridad Informática de SERVAGRO LTDA, emerge como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la empresa cumplir con su misión.

El proponer esta Política de Seguridad requiere un alto compromiso con la empresa, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

5 POLÍTICAS DE SEGURIDAD

La oficina de SISTEMAS actualmente está conformado por 1 funcionario el cual cumple distintas funciones referentes al soporte y mantenimiento de la plataforma tecnológica, desarrollo de sistemas de información, administración de bases de datos, gestión de recursos de tecnología y administración de la red, dado a esta razón ha sido necesario emitir políticas particulares para el conjunto de recursos y facilidades informáticas de la infraestructura de telecomunicaciones y servicios asociados a ellos, provistos por la oficina de SISTEMAS. Así este apartado contiene una clasificación de estas políticas y son:


5.1 Equipos de cómputo

5.1.1 De la instalación del equipos de cómputo

1. Todo equipo de cómputo llámese: Computadoras, estaciones de trabajo, servidores y/o equipos accesorios, que este o sea conectado a la red de Servagro, o aquel que en forma autónoma se tenga y que sea propiedad de la empresa debe de sujetarse a las normas y procedimientos de instalación que emite el departamento de SISTEMAS.
2. La oficina de SISTEMAS en coordinación con el área de ALMACÉN y CONTABILIDAD, deberá tener un registro de todos los equipos de propiedad de la empresa.
3. El equipo de la empresa que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de seguridad física, condiciones ambientales, alimentación eléctrica y la normatividad para el acceso de equipos, que la oficina de SISTEMAS implante.
4. El funcionario de la oficina de SISTEMAS debe dar cabal cumplimiento con las normas de instalación y notificaciones correspondientes de actualización, reubicación, reasignación y todo aquello que implique movimientos en ubicación de adjudicación, sistema y misión.
5. La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, al departamento de SISTEMAS.

5.1.2 Del mantenimiento del Equipo de Computo

1. La oficina de SISTEMAS corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.
2. En caso de los equipos sean atendidos por terceros la oficina de SISTEMAS, deberá coordinar y velar por el cuidado y preservación del mismo.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

3. Los responsables de las áreas de cómputo de un departamento pueden otorgar mantenimiento preventivo y correctivo, a partir del momento en que sean autorizados por el área de SISTEMAS.
4. Corresponde al área de SISTEMAS y debe dar a conocer las listas de las personas que pueden tener acceso a los equipos y brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.
5. Por motivos de normatividad interna de SERVAGRO LTDA, comunica queda que estrictamente prohibido dar mantenimiento a equipos de cómputo que no es propiedad de la empresa.

5.1.3 De la actualización del equipo de cómputo

1. Todo equipo de computo (computadoras personales, estaciones de trabajo y demás relacionados) y los de telecomunicaciones que sean de SERVAGRO LTDA. Debe procurarse que sea actualizado tendiendo a conservar e incrementar la calidad del servicio que se presta, mediante la mejora sustantiva de su desempeño.


5.1.4 De la reubicación del equipo de cómputo

1. La reubicación del equipo de cómputo se realizara satisfaciendo las normas y procedimientos que el área de SISTEMAS emita para ello.
2. En caso de existir personal técnico de apoyo, este notificara de los cambios tanto físicos como de software que realice. Dando aviso a la oficina de SISTEMAS y al área de ALMACÉN, notificando también los cambios de los equipos para adjuntarlos al inventario.
3. El equipo de cómputo a reubicar sea de un tercero o bien sea externo se hará únicamente bajo la responsabilidad y contando con la presencia de la persona, se reubicara con los medios necesarios para la instalación del equipo.

5.2 Control de accesos

5.2.1 Del acceso a Áreas Críticas

1. El acceso de personal se llevara acabo de acuerdo a las normas y procedimientos que dicta la oficina de SISTEMAS.
En concordancia con la política de la empresa y debido a la naturaleza de estas áreas se llevara un registro permanente del tráfico de personal, sin excepción.
2. La oficina de SISTEMAS deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.
3. Bajo condiciones de emergencia o de situaciones de urgencia manifestada, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la empresa.

	SERVAGRO LTDA	Fecha.	19 Enero 2015
		Versión.	1.2.5
	Sección: Seguridad y Control	Cód.	XXXXX

5.2.2 Del control de acceso al equipo de computo


1. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos de la oficina de SISTEMAS emita.
3. Las áreas donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítico, deberán sujetarse también a las normas que establezca la oficina de SISTEMAS.
4. Los accesos a las áreas críticas deberán de ser clasificados de acuerdo a las normas que la oficina de SISTEMAS, de común acuerdo con las autoridades de la empresa emitan para ello.
5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la oficina de SISTEMAS, tiene la faculta de acceder a cualquier equipo de cómputo que no esté bajo supervisión.

5.2.3 Del control de acceso local de la red

1. La oficina de SISTEMAS es la responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
2. La oficina de SISTEMAS es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.
3. Dado el carácter unipersonal del acceso a la red de SERVAGRO LTDA, la oficina de SISTEMAS verificara el uso responsable de acuerdo al reglamento para el uso de la red.
4. El acceso lógico a equipos especializados (Servidores, enrutadores, bases de datos, equipos de súper computo centralizado y distribuidor, etc.) conectado a la red es administrado por la oficina de SISTEMAS.
5. Todo equipo de cómputo que este o sea conectado a la red de SERVAGRO LTDA, o aquellas que en forma autónoma se entregan y que sean propiedad de la empresa, debe de sujetarse a los procedimientos de acceso que emite la oficina de SISTEMAS.

5.2.4 Del control de acceso remoto

1. La oficina de SISTEMAS es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos.
2. Para el caso especial de los recursos de SERVIDORES a terceros deberán ser autorizados por la DIRECCION GENERAL o por la oficina de TALENTO HUMANO.
3. El uso de estos servicios deberá sujetarse al Reglamento de uso de la red de SERVAGRO LTDA. Y en concordancia con los lineamientos generales de uso de internet.
4. El acceso remoto que realicen personas ajenas a la empresa deberá cumplir las normas que emite la oficina de SISTEMAS.


	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

5.2.5 Del acceso a los sistemas administrativos

1. Tendrá acceso a los sistemas administrativos solo el personal de SERVAGRO LTDA. O personas que tenga la autorización por la DIRECCIÓN GENERAL DE LA EMPRESA.
2. El manejo de información administrativo que se considere de uso restringido deberá ser cifrado con el objetivo de garantizar su integridad.
3. Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquier persona, excepto para la persona de la oficina de SISTEMAS.
4. El control de acceso a cada sistema de información de la Dirección Administrativa será determinado por la unidad responsable de generar y procesar los datos involucrados.

5.2.6 De las WWW

1. En concordancia con la LEY 1273 y de común acuerdo con las políticas generales de informática, la oficina de SISTEMAS, es el responsable de instalar y administrar el o los servidor(es) WWW. Es decir, solo se permiten servidores de páginas autorizadas por la oficina de SISTEMAS.
2. La oficina de SISTEMAS deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la intranet empresarial, así como las especificaciones para que el acceso a estos sea seguro.
3. Los accesos a las páginas Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la red de SERVAGRO LTDA.
4. A los responsables de los servidores Web corresponde la verificación de respaldo y protección adecuada.
5. Toda la programación involucrada a la tecnología Web deberá estar de acuerdo con las normas y procedimientos que la oficina de SISTEMAS, emita.
6. El material que aparezca en la página de internet de SERVAGRO LTDA, deberá ser respaldado por la oficina de SISTEMAS, respetando la ley de propiedad intelectual, (Derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).
7. En concordancia con la libertad de investigación, se acepta que en la red de SERVAGRO LTDA. Conectada a internet pueda ponerse información individual sin autorización, (Siempre y cuando no contravenga las disposiciones que se aplican a las instituciones gubernamentales para estatales).
8. Con referencia a la seguridad y protección de las páginas Web, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por la oficina de SISTEMAS.
9. La oficina de SISTEMAS, tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información y conservar información del tráfico.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

5.3 Utilización de los recursos de la red

1. Los recursos disponibles a través de la Red de SERVAGRO LTDA. Serán de uso exclusivo para asuntos relacionados con las actividades de la empresa.
2. La oficina de SISTEMAS, es la responsable de emitir y dar seguimiento al Reglamento para el uso de la Red.
3. La oficina de SISTEMAS, debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices económicas y ecológicas de la empresa.


5.4 Del software

5.4.1 De la adquisición del software

1. En concordancia con la política de la empresa y la oficina de SISTEMAS, son los organismos oficiales de la empresa para establecer los mecanismos de procuración de sistemas informáticos.
2. Del presupuesto de los proyectos que se otorga a las diferentes áreas de SERVAGRO LTDA. Una cantidad deberá ser aplicada para la adquisición de sistemas informáticos, licencias o el desarrollo de sistemas de información a la medida.
3. De acuerdo con el MINISTERIO DE LAS TI, la dirección General en conjunto con la oficina de SISTEMAS, propiciara la adquisición de licencias de sitio, licencias flotantes, licencias de software libre, licencias por empleado y de licencias en cantidad, para obtener economía de escala y de acorde al plan de austeridad del gobierno de la república.
4. Corresponderá a la oficina de SISTEMAS, emitir para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.
5. De acuerdo a los objetivos globales de la oficina de SISTEMAS, deberá propiciar la adquisición y asesoramiento en cuanto al software de vanguardia.
6. En cuanto a la paquetería sin costo respetándose la propiedad intelectual intrínseca del autor.
7. La oficina de SISTEMAS, promoverá y propiciara que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
8. La oficina de SISTEMAS, deberá promover el uso de sistemas programáticos que redunden en la independencia de la empresa con los proveedores.

5.4.2 De la instalación del software

1. Corresponde a la oficina de SISTEMAS, emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.
2. En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.
3. Los departamentos que posean un equipo de cómputo y manejen información, son los responsables de brindar asesoría y supervisión para la instalación necesaria de

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

software informático, así mismo la oficina de SISTEMAS, se asesorara del software de telecomunicaciones.

4. La instalación de software que desde el punto de vista de la oficina de SISTEMAS, pudiera poner en riesgo los recursos de la empresa no está permitida.
5. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad, (Antivirus, vacunas, privilegios de acceso y otros que se apliquen).
6. La protección lógica de los sistemas corresponde a quienes en un principio se les asigna el equipo de cómputo y les compete notificar cualquier movimiento a la oficina de SISTEMAS.

5.4.3 De la actualización del software


1. La adquisición y actualización de software para el equipo especializado de telecomunicaciones, se llevara a cabo de acuerdo a la calendarización que anualmente sea propuesta por la oficina de SISTEMAS.
2. Corresponde a la oficina de SISTEMAS, autorizar cualquier adquisición y actualización del software.
3. Las actualizaciones del software de uso común o más generalizado se llevara de acuerdo al plan de actualización desarrollado por la oficina de SISTEMAS.

5.4.4 De la auditoria del software instalado

1. El área de CONTROL INTERNO de SERVAGRO LTDA. Es el responsable de realizar revisiones periódicas para asegurar que solo programación con licencia este instalada en las computadoras de la empresa.
2. El área de CONTROL INTERNO y la oficina de SISTEMAS, propiciara la conformación de un grupo especializado en auditoria de sistemas de cómputo y sistemas de información.
3. Corresponderá al grupo especializado dictar las normas, procedimientos y calendarios de auditorio.

5.4.5 Del software de propiedad de la empresa

1. Toda programación adquirida por la empresa sea por compra, donación o cesión es propiedad de la empresa y mantendrá los derechos que la ley de propiedad intelectual le confiera.
2. La oficina de SISTEMAS, en coordinación con el área de CONTABILIDAD, deberá tener un registro de todos los paquetes de programación.
3. Todos los sistemas programáticos, (Programas, bases de datos, sistemas operativos e interfaces), desarrollados con o a través de los recursos de SERVAGRO LTDA, se mantendrán como propiedad de la empresa, respetando la propiedad intelectual del mismo.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

4. Es obligatorio de todos que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como activo de la empresa que debe preservarse.
5. Los datos, bases de datos, la información generada por el personal y los recursos informáticos de la empresa deben estar resguardados.
6. Corresponderá a la oficina de SISTEMAS, promover y difundir los mecanismos de respaldo, salvaguardar de los datos y de los sistemas programáticos.
7. La oficina de SISTEMAS, administrara los diferentes tipos de licencias de software y vigilara su vigencia en concordancia con la política informática.

5.4.6 De la propiedad intelectual


1. Corresponde a la oficina de SISTEMAS, procurar que todo el software instalado en SERVAGRO LTDA, este de acuerdo a la ley intelectual a que dé lugar.

5.5 Supervisión y evaluación

1. Las auditorias de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca la oficina de SISTEMAS y/o el grupo especializado de seguridad.
2. Para efectos de que la empresa disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la internet e intranet disponen.
3. Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.


5.6 Copias de seguridad y Backups

1. La oficina de SISTEMAS, estará encargado de colocarles una carpeta directa a un servidor el cual es el encargado de realizar las copias de seguridad.
2. Cada usuario encargado de la información de la empresa de SERVAGRO LTDA, está obligado a colocar su información a esta carpeta y posteriormente será extraída para ser resguardada en la bóveda.
3. Todas las carpetas se les sacaran copias de seguridad y serán guardadas en discos duros, discos de DVD, cintas magnéticas o que dé lugar al caso.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX


6 GENERALES

1. Cada uno de los departamentos deberá de emitir los planes de contingencia que correspondan a las actividades críticas que realicen.
2. Debido al carácter confidencial de la información, el personal de la oficina de SISTEMAS, deberá de conducirse de acuerdo a los códigos de ética profesional, normas y procedimientos establecidos.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX


7 SANCIONES

1. Cualquier violación a las políticas y normas de seguridad deberá ser sancionado de acuerdo al reglamento emitido por la SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA.
2. Las sanciones pueden ser desde una llamada de atención, suspensión o informar al usuario la suspensión del servicio, dependiendo de la gravedad de la falta y de la malicia o perversidad que esta manifiesta.
3. Corresponde al grupo de informática, hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la empresa.
4. Todas las acciones en las que se comprometa la seguridad de la red de SERVAGRO LTDA, y que no estén previstas en esta política, deberán ser revisadas por la Dirección General, para dictar una resolución sujetándose al estado de derecho.
5. En cuanto a los daños de la infraestructura tecnológica, interceptación ilegítima de sistema informático, sobre la red, sistema de telecomunicaciones, suplantación de sitios web para capturar datos personales, acceso abusivo a un sistema informático y de más delitos informáticos se aplica la LEY 1273, incurriendo a las sanciones que aplica.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

8 RECOMENDACIONES

1. Se tendrá que convocar al GRUPO DE ESPECIALISTAS EN INFORMATICA a nivel de la alta gerencia, la cual provea soluciones informáticas y tecnológicas, promoviendo la preservación de la arquitectura tecnológica de la empresa y la información vital de la misma.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

9 PLAN DE CONTINGENCIA INFORMÁTICO

La protección de la información vital de una empresa ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático.

Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. Por lo anterior es importante contar con un Plan de contingencia adecuado de forma que ayude a la Entidad a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio.

9.1 Introducción


Para realizar el Plan de contingencia informático de SERVAGRO LTDA, se tiene en cuenta la información como uno de los activos más importantes de la Empresa, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la Empresa. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.). El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

Es importante resaltar que para que este Ente de Control logre sus objetivos es indispensable el manejo de información, por tanto necesita garantizar tiempos de indisponibilidad mínimos para no originar distorsiones al funcionamiento normal de nuestros servicios y mayores costos de operación, ya que de continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar las operaciones por falta de información para el control y toma de decisiones de la entidad. De acuerdo a lo anterior es necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo mejor posible.

9.2 Objetivos

- Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

proteger la Información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

- Garantizar la continuidad de las operaciones de los principales elementos que componen los Sistemas de Información.

Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

9.3 Identificación de procesos y servicios

9.3.1 Principales Procesos de Software Identificados


1. Software
 - A. Presupuesto.
 - B. Contabilidad.
 - C. Tesorería.
 - D. Almacén.
 - E. Responsabilidad fiscal.
 - F. Cobro coactivo.

9.3.2 Principales servicios que deberán ser restablecidos Y/O recuperados

1. Windows
 - A. Correo electrónico
 - B. Internet
 - C. Antivirus
 - D. Herramienta de Microsoft Office
2. Software Base
 - A. Base de datos.
 - B. Backup de la Información.
 - C. Ejecutables de las aplicaciones.
3. Respaldo de la Información
 - A. Backup de la Base de Datos.
 - B. Backup de la Plataforma de Aplicaciones (Sistemas).
 - C. Backup de la WEBSITE.
 - D. Backup del Servidor.

9.4 Minimización del riesgo

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo. Es de tener en cuenta que en lo que respecta a Fenómenos naturales, nuestra región ha registrado en

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

estos últimos tiempos movimientos telúricos de poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios, techos, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

9.4.1 Incendio o Fuego

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Aleatorio

Grado de Impacto: Alto

Situación Actual	Acción Correctiva
La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma cada piso cuenta con un extintor con capacidad y cargado.	Se cumple
No se ha ejecutado un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a los funcionarios nuevos, lo que no es eficaz para enfrentar un incendio y sus efectos	Realizar capacitación para el manejo de extintores y primeros auxilios.
El servidor realiza backups de la información diariamente, pero no existe ninguna otra copia de respaldo.	Realizar backups del servidor de forma mensual, almacenada en Disco Duro y ubicada en la bóveda de la Empresa.

Analizando el riesgo de incendio, permite resaltar el tema sobre el lugar donde almacenar los backups. El incendio, a través de su acción calorífica, es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD's, DV's, cartuchos, Discos duros. Para la mejor protección de los dispositivos de almacenamiento, se colocaran estratégicamente en lugares distantes, cerca a la salida de la empresa.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos cerca del las posibles áreas de riesgo que se debe proteger.


9.4.2 Robo Común de Equipos y Archivos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Moderado

Situación Actual	Acción Correctiva
Debido a que a la hora de salida de las personas particulares que ingresan a la empresa, no son registradas. Cabe anotar que contamos con sistema de seguridad.	Se requiere que cada funcionario en el momento de retirarse de la oficina por un tiempo considerable, opte por guardar su equipo dentro de algún cajón bajo llave.

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

Autorización escrita firmada por el Jefe de área, Responsable de sistemas y funcionario responsable, para la salida de equipos de la Entidad.	Se cumple por medio del formato establecido para salida de equipos.
Por la ubicación de la Empresa existe riesgo de hurto a mano armada.	Solicitar la colaboración de la Policía Nacional para que realice rondas periódicas por el sector donde se encuentra ubicada la empresa.

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización del Jefe de Cada Área y la persona de Sistemas, esto demuestra que los equipos se encuentran protegidos por cada funcionario autorizado.


Según antecedentes de otras empresas, es de conocer que el robo de accesorios y equipos informáticos, llegaron a participar personal propio de la empresa en colusión con el personal de vigilancia, es relativamente fácil remover un disco duro del CPU, una disquetera, tarjeta, etc. y no darse cuenta del faltante hasta días después. Estas situaciones no se han presentado en nuestro Ente de Control, pero se recomienda siempre estar alerta

9.4.3 Falla en los Equipos

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Grave

Situación Actual	Acción Correctiva
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de quipos que están para dar de baja.
Cada área funcional se une a la Red a través Gabinetes, la falta de energía en éstos, origina la ausencia de uso de los servicios de red	Se cumple. Los gabinetes se encuentran protegidos en un lugar de acceso restringido y son manipulados solo por la persona de sistemas.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Se cumple. Cuentan con portátiles por tanto se recomienda que cada funcionario mantenga cargado su equipo y los de escritorio se cuenta con UPS.

Teniendo en cuenta la importancia del fluido eléctrico para el funcionamiento de la entidad, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas

	SERVAGRO LTDA	Fecha. 19 Enero 2015
		Versión. 1.2.5
	Sección: Seguridad y Control	Cód. XXXXX

gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos. El equipo de aire acondicionado y ambiente adecuado en el Área de Servidores, favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales de escritorio, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del Hardware y la información podría perderse. La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico.

9.4.4 Fenómenos Naturales

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Situación Actual	Acción Correctiva
En la última década no se han registrado urgencias por fenómenos naturales como terremotos o inundaciones.	Aunque la probabilidad de ocurrencia es baja se requiere tener en cuenta medidas de prevención.
Aunque existen épocas de lluvia fuertes, la empresa está debidamente protegida.	Tomar medidas de prevención
Los servidores principales se encuentran en un ambiente libre de filtraciones.	Ante la mínima filtración se debe informar de inmediato a la dirección, para realizar el respectivo mantenimiento preventivo.

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos necesarios en la sala de Computación, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.