CENABASTOS S.A.
¡Sembrando el futuro!

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

CENABASTOS S.A., en cumplimiento de la Política Nacional de Seguridad digital del Ministerio de Tecnologías de la Información y las Comunicaciones contenida en el documento CONPES 3854 aprobada el 11 de abril de 2016, define el esquema para garantizar la seguridad y calidad de la información que maneja y medio de distribución de productos y servicios para clientes y usuarios; para ello ha elaborado en este documento de manual de políticas de seguridad de la información, a fin de que sean aplicables por todo el personal de planta y contratistas, que acceden a activos de información de la Sociedad, quienes tendrán conocimiento de la importancia de la información y servicios críticos, los riesgos y nuevas amenazas a que están expuestos.

Estas políticas serán divulgadas formalmente a todos los funcionarios y se establecerá mecanismos de seguimiento y control, sobre el conocimiento y aplicación de las mismas.

Las políticas incluidas en este Manual se constituyen como parte fundamental para el cumplimiento de la misión y visión de CENABASTOS S.A. y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La Seguridad de la Información es una prioridad para CENABASTOS S.A. y por tanto es responsabilidad de todos velar por que no se realicen actividades que vayan en contra del fundamento de cada una de estas políticas.

CENABASTOS S.A.
¡Sembrando el futuro!

OBJETIVO

Establecer dentro del Programa de Gestión Documental- PGD-, las políticas, medidas de seguridad y mecanismos de control que permitan proteger, asegurar y garantizar la confidencialidad, autenticidad, integridad, disponibilidad y confiabilidad de los activos de información de CENABASTOS S.A.

ALCANCE

Las Políticas de Seguridad de la Información de CENABASTOS S.A. presentadas por este manual, se aplica a todos los activos de información de la entidad, durante su ciclo de vida, incluyendo creación, distribución, trasmisión, almacenamiento y eliminación; están orientadas a proteger los activos de información en todos los ambientes en los cuales reside y a asegurar que estén sometidos a controles equivalentes para su protección.

Las Políticas y Normas de Seguridad de la información son aplicables a la administración de:

• La información: Datos almacenados en cualquier medio magnético y físico.

• El software: Sistemas operacionales, programas, productos y aplicaciones.

• El hardware: Equipos de cómputo, telecomunicaciones y redes.
• Las Personas: Usuarios y Administradores de la información, ya sean los empleados, contratistas y terceros que prestan servicios a la entidad.

• Procesos: Las Políticas y Normas de Seguridad de la información cubren todas las operaciones y funciones que se apoyen en sistemas de información.

OBJETIVOS ESPECÍFICOS

• Dar a conocer las Políticas y procedimientos de Seguridad de la información, las cuales serán de obligatorio cumplimiento en el desarrollo de las actividades de los empleados, contratistas y terceros que prestan servicios a la entidad. , así mismo, operaciones de cómputo, Telecomunicaciones, Redes y desarrollo de Sistemas de Información de CENABASTOS S.A.

• Determinar los mecanismos de protección necesarios que garanticen el funcionamiento óptimo de los recursos informáticos de la organización.

• Establecer las labores de seguridad y vigilancia de las diferentes dependencias de CENABASTOS S.A.

• Establecer las medidas de seguridad para los terceros que tienen algún tipo de convenio con el manejo y/o administración de los activos de información de la organización.

• Divulgar y capacitar a los funcionarios de CENABASTOS S.A., sobre el presente manual de acuerdo a sus funciones y responsabilidades.

MARCO CONCEPTUAL

La seguridad de Información se refiere al establecimiento de las medidas organizacionales, técnicas y sociales, necesarias para proteger los activos de información: hacking informático, divulgación, duplicación, intercepción, modificación, destrucción, pérdida, supresiones, daños, deterioros, robo, mal uso, interrupción de sistemas, etc., que se pueda producir en forma intencional o accidental.

REFERENCIAS NORMATIVAS

• Ley 1266 de 2008 “Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información”.

• Ley 1273 de 2009 “Protección de la Información y de los Datos”.

• Documento CONPES 3701 de julio del 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”.

• Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.

• Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.

•Norma Técnica Colombiana NTC – ISO/IEC 27000.

TERMINOLOGÍA Y DEFINICIONES DE CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN

• Activo de información: Es todo aquel recurso tangible o intangible que tenga VALOR o IMPORTANCIA para la organización, de acuerdo a la tipificación definida.

• Confidencialidad: Consiste en garantizar que el activo de información no esté disponible o sea divulgado por personas, entidades o procesos NO autorizados.

• Integridad: Consiste en asegurar o salvaguardar que el activo de información cuente con las propiedades de: exactitud, precisión, consistencia, confiablidad y totalidad.

• Disponibilidad: Consiste en garantizar que el activo de información este accesible y utilizable en el momento oportuno que se requiera bajo la demanda de personas, entidades o procesos.

• Autenticidad: Consiste en garantizar que las personas, entidades o procesos sean lo que dicen ser ante un activo de información.

• Autorización: Es el otorgamiento de permiso a una persona, entidad o proceso, para acceder a un activo de información.

• No-Repudiación: Consiste en asegurar que el activo de información NO sea negado bajo un evento o transacción demandado por personas, entidades o procesos.

• Adaptabilidad: Permite identificar y rastrear toda operación llevada a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados.

• Trazabilidad: Asegurar que en todo momento se podrá determinar quién accedió a qué activo de información (servicio, datos, etc.), qué hizo y en qué momento lo hizo.

• Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

• Eficiencia: Criterio de calidad en que el procesamiento y suministro de la información, que debe contar con la capacidad de lograr ese efecto con el mínimo de recursos posibles o en el menor tiempo posible.

• Archivos: Conjunto de datos o instrucciones que se almacenan en el Disco Duro y/o cualquier otro medio de almacenamiento con un nombre que los identifica.

• Autorización: Proceso o procedimiento oficial, por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información o activos físicos.

• Backup: Copiar y resguarda la información para protegerla de posibles riesgos.

• Contraseña (Password): Clave para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc. Esta clave debe ser personal e intransferible y no se debe anotar en documentos físicos de fácil acceso.

• Cuenta de Usuario: Es el identificador que utiliza un Sistema de Información en la autenticación de un usuario.

• Cuenta de Correo: Servicio en línea que provee un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico en Internet.

• Equipos de cómputo: Dispositivo electrónico que se emplea para procesar datos. También pueden ser considerados como equipos de cómputo los equipos que prestan servicios de almacenamiento y procesamiento desde la nube.

• Hardware: Partes físicas de un sistema de procesamiento de datos.

• Incidente: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política.

• Información: Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

• Log: Archivo que registra movimientos y actividades de un determinado programa, utilizado como mecanismo de control y estadística.

• Medios de almacenamiento externo: Medio utilizado para el almacenamiento de información, que puede conectarse o introducirse y retirarse del Hardware por varias interfaces como puertos USB, unidad de cinta, unidades de disco, etc.

• Parche de Seguridad: Conjunto de instrucciones de corrección para un software en especial, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento, en el código original de este.

• Periféricos: Dispositivo electrónico físico que se conecta o acopla a una computadora, pero no forma parte del núcleo básico.

• Recursos informáticos: Software y hardware.

• Red: Nombre dado al conjunto de equipos de cómputo y de telecomunicaciones, interconectados entre sí al interior de la organización, para permitir a los usuarios acceso a los recursos tecnológicos.

• Software: Es el conjunto de instrucciones mediante las cuales el Hardware puede realizarlas tareas ordenadas por el usuario. Está integrado por los programas, sistemas operativos y utilidades.

• Software ilegal: Es el Software que se adquiere y se instala sin el consentimiento de la empresa que lo desarrolla o sin licencia de uso.

CENABASTOS S.A.
¡Sembrando el futuro!

TERMINOLOGÍA Y DEFINICIONES PARA EL ESTUDIO DE LOS RIESGOS Y CONTROLES A LA SEGURIDAD DE LA INFORMACIÓN.

• Riesgo: Es la posibilidad que una amenaza explote o penetre una vulnerabilidad de un activo de información, impactando a este activo de información y/o activos asociados, viéndose afectando del mismo modo los objetivos del negocio.

• Gestión del riesgo: Actividades coordinadas para dirigir y controlar los activos de información de la organización con respecto al riesgo, para cada uno de sus procesos, subprocesos o áreas funcionales. La importancia de la administración del riesgo se basa en la:

- Necesidad de cumplir con un número creciente de disposiciones regulatorias.

- Necesidad de responder rápida y efectivamente a los cambios y riesgos del entorno de los negocios.

- Necesidad de asegurar la sustentabilidad de los negocios en el tiempo.

- Mejora continua a través de controles que disminuyan las vulnerabilidades, fallas, consecuencias ante la probabilidad de impacto.

• Análisis del riesgo: Se basa en la revisión y evaluación sistemática de la información para identificar las fuentes y estimación del riesgo a través de las causas de las posibles amenazas y probables de eventos no deseados y los daños y consecuencias que éstas puedan producir. La medición y evaluación continua de amenazas, impacto y vulnerabilidades sobre los activos de información que permitan la minimización de la ocurrencia de dichos riesgos de seguridad, esto se realiza a través del PHVA.

• Incidente de seguridad de la información: Se considera un Incidente de seguridad de la Información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

• Vulnerabilidad: Es una debilidad de seguridad asociada a un activo de información que puede hacer que una amenaza se haga efectiva.

Para cada vulnerabilidad se debe medir la criticidad de la probabilidad de ocurrencia de la misma, bajo los siguientes criterios.

• Amenaza: Es la indicación de un potencial evento no deseado que afecte negativamente la confidencialidad, integridad, disponibilidad o confiabilidad de los activos de información y que expone de alguna manera la entidad.

• Autenticación fuerte: Esquema de autenticación mediante el cual el sujeto que se identifica debe utilizar por lo menos dos de tres posibles factores. Los Factores pueden ser algo que se tiene, tal como una tarjeta de proximidad; algo que se sabe, como una clave personal (contraseña); algo que se es, es decir, una característica única inherente a la persona, como la huella digital.

• Cifrado fuerte: Técnicas de codificación para protección de la información que utilizan algoritmos de robustez reconocidos internacionalmente, brindando los niveles de seguridad ofrecidos.

• Control: Una forma para manejar el riesgo, en la cual se incluyen políticas, procedimientos, estructuras organizacionales y elementos tecnológicos, que pueden ser de carácter administrativo, técnico, procedimental o legal.

• Continuidad: Es la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

• Propietario activo de información: Área o persona que tiene la responsabilidad de clasificar y definir el grado de seguridad que se debe aplicar a un activo de información, autorizar el acceso y velar por que se implementen controles que disminuyan el riesgo por pérdida de la integridad, confidencialidad y disponibilidad del mismo.

ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

A continuación se describen algunas acciones identificadas que afectan la Seguridad de la Información, y que ponen en riesgo su disponibilidad, confidencialidad e integridad:

1. Dejar los computadores encendidos en horas no laborables.

2. Permitir que personas ajenas a la Sociedad ingresen sin previa autorización a las oficinas o donde se procese información sensible.

3. No clasificar y/o etiquetar la información.

4. No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.

5. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.

6. Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.

7. Hacer uso de la red de datos o de la página web de la Sociedad para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.

8. Instalar softwares cuyo uso no esté autorizado y que puedan atentar contra las leyes de derechos de autor o propiedad intelectual.

9. Enviar información clasificada de la Sociedad por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.

10. Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la Sociedad.

11. Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la Sociedad sin la debida autorización.

12. Ingresar a la red de datos de Sociedad por cualquier servicio de acceso remoto sin la autorización.

13. Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos de la Sociedad para beneficio personal.

14. Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario o contratista.

15. Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.

16. Retirar de las instalaciones de la Sociedad computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.

17. Entregar, enseñar o divulgar información clasificada de la Sociedad a personas o entidades no autorizadas.

18. Llevar a cabo actividades ilegales, o intentar acceso no autorizado a los softwares, correos electrónicos institucionales o página web de la Sociedad o de terceras partes.

19. Ejecutar cualquier acción que difame, afecte la reputación o imagen de la Sociedad, o alguno de sus funcionarios, utilizando para ello los softwares, correos electrónicos institucionales o página web.

20. Realizar cambios no autorizados en los softwares, correos electrónicos institucionales o página web de la Sociedad.

21. Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.

22. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de Seguridad de la Información.

23. Consumir alimentos y bebidas, cerca del área de archivo.

24. Conectar a la corriente regulada dispositivos diferentes a equipos de cómputo.

25. Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

CENABASTOS S.A.
¡Sembrando el futuro!

POLITICAS GENERALES

1. Finalización De La Relación Laboral

Al momento de la desvinculación o cambio de roles en la Sociedad, todo funcionario o contratista debe hacer entrega de todos los activos de información que le hayan sido asignados.

2. Gestión De Incidentes De Seguridad De La Información

a. Los funcionarios y contratistas de la Entidad deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

b. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.

3. Derechos de Propiedad Intelectual

a. No se permitirá el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

b. Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

c. Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

d. El desarrollo de software a la medida adquirido a terceras partes o realizados por funcionarios de la Sociedad, serán de uso exclusivo Cenabastos S.A. y la propiedad intelectual será de quien lo desarrolle.

3. Uso De Correo Electrónico

• Todos los mensajes enviados por medio de correo electrónico pertenecen a IDIGER, el cual se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.

• Es responsabilidad del Usuario enmarcar todos los mensajes que envíe a través de correo electrónico dentro de las normas mínimas de respeto y protocolo electrónico, sin incluir contenidos hostiles que molesten a los receptores del mismo, tales como comentarios sobre sexo, raza, religión o preferencias sexuales, tendencia política entre otras que generen algún tipo de discriminación; así mismo, es responsabilidad del usuario reportar al Jefe de área la recepción de este tipo de mensajes.

• Es responsabilidad del Usuario evitar que su cuenta de correo electrónico sea utilizada por terceros.

• Es responsabilidad del Usuario evitar que la información confidencial y/o sensible sea transmitida por medio de su cuenta de correo electrónico, salvo autorización previa y escrita del dueño de la información.

• Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

• Es responsabilidad del Usuario eliminar periódicamente de sus dispositivos de almacenamiento los mensajes que ya no necesite. Con esto se reducen los riesgos de que otros usuarios puedan acceder a esa información; y además, se libera espacio en disco.

TIPOS DE ATAQUES Y ATACANTES

• Hoax (correos falsos).- Es un mensaje de correo electrónico con contenido falso o engañoso. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante, a que parece provenir de una fuente seria y fiable o porque el mismo mensaje pide ser reenviado.

• Phishing (Pesca).- Es el acto de pescar usuarios mediante señuelos y de este modo obtener información financiera y contraseñas para intentar adquirir información confidencial de forma fraudulenta.

• Spoofing (suplantación de identidad).- Es una técnica que consiste en hacer creer al receptor de un mensaje de correo electrónico, que quien remite el mensaje es alguien de confianza. El verdadero emisor queda suplantado por una dirección real, que ofrece garantías al receptor, que abrirá ingenuamente el mensaje sin conocer los verdaderos motivos (ocultos).

• Spammers.- Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido; habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.

• Spamblock. Texto que se inserta en una dirección de correo electrónico ocultando la verdadera dirección, cuyo objetivo es burlar a los spammers. Por ejemplo, si mi dirección de correo es grupo@compañiaf.com.co, mediante esta técnica se puede transformar en grupo@rcompañiaf.com.co.

• Crimeware.- Es un software diseñado específicamente para cometer delitos financieros en entornos en línea, técnicas mediante la ingeniería social u otras técnicas genéricas de fraude en línea. El objetivo es robar identidades en línea para acceder a los datos financieros de un usuario, con el fin de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el crimeware.

• Malware (Software malicioso).- Es un tipo de software que tiene como objetivo infiltrarse o dañar un Pc sin el consentimiento de su dueño.

• Virus.- Es un software que se copia por sí mismo, infecta un Pc, se propaga dentro de todo los archivos, luego se copia de Pc a Pc; estos virus se adhieren en archivos específicos (de arranque, script, macros o ejecutables); el fin de este software es alterar o corromper el funcionamiento normal de un Pc.

• Spyware.- Es un software cuyo objetivo es mandar información a un tercero de toda las páginas visitadas; el fin es espiar y recabar información de las páginas a las cuales fueron visitadas (incluyen claves de cuenta, correos, etc.) para luego en lo posterior, enviar o saturar de publicidades. La recolección de esta información es mediante un canal falso, produciendo un consumo de ancho de banda de internet y a su vez poniendo lento el computador.

• Gusano.- Es un software cuyo único cometido radica en pasar de Pc en Pc a través de redes informáticas en forma automática sin la intervención de ningún usuario; estos normalmente buscan traspasar los agujeros de seguridad para infectar toda la red a su alcance.

• Adware.- Se trata de un software que permite publicidad no deseada vía Internet y que generalmente se instala sin nuestro consentimiento.

• Scareware (Software de miedo).- Es un software que engaña a un usuario para descargar un programa haciendo creer que está infectado de virus; es un método de estafa para hacer comprar un software utilizando prácticas comerciales poco éticas.

• Caballo de Troya.- Es un software inocente que contiene códigos escondidos que permiten la modificación no autorizada y la explotación o destrucción de la información. Los troyanos se distribuyen por Internet, juegos, protectores de pantalla y crack de programas.

• Botnet.- Son redes de computadoras infectadas, también llamadas "zombies", que pueden ser controladas a la vez por un individuo y realizan distintos ataques (envío masivo de spam o para lanzar ataques DDos). El fin de este ataque puede ser de extorsión, impedir su correcto funcionamiento, etc.

• Rogue software.- Software que hace creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso; esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.
• Hijacking.- Es una técnica ilegal que tiene por objetivo el adueñarse o robar (TCP/IP, página web, dominio, navegadores, módems, temas de foros, sesiones de terminal, servicios etc.) mediante una conexión de red.

• Carding.- Uso ilegítimo de las tarjetas de crédito ajenas, generar números de tarjetas de crédito y cualquier otra actividad ilegal relacionada con las mismas.

• Trashing.- Se trata de buscar en la basura (física o informática) información que pueda ser útil para realizar fraudes, copias, suplantaciones, etc.

• Graffiti. Modificación que un hacker hace de la página web de un servidor para evidenciar la falta de protección de un sistema.

• Defacement.- Hace referencia a la deformación o cambio de manera intencionada a una página web, ya sea por venganza, diversión o burla; esto se debe a algún error de programación de la página por algún bug en el propio servidor o por una mala administración de este.

• Phreaking.- Son individuos que orientan sus estudios u ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas y sistemas que componen una red telefónica, electrónica aplicada a sistemas telefónicos.

• Cracker.- Son individuos que se dedican a desproteger programas, como evitar tener que pagar las licencias de los mismos, comprar una copia y usarla en 20 puestos simultáneamente.

• Hacker.- Persona que es capaz de eludir los sistemas de seguridad de un computador para acceder a la información que contiene ya sea con fines maléficos o benéficos.

• Hacktivista.- Persona especialista que se moviliza con conocimientos informáticos contra la mundialización, las multinacionales y en defensa de los internautas.

• Ankle-Biter (packet-monkeys, script kiddies o crashers) Son personas que indagan por la red ya sea por diversión o pasa tiempo para realizar ataques sólo para divertirse, sin importar quién los recibe.
• Rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

OBLIGATORIEDAD

El Manual de Políticas de Seguridad de la Información es de obligatorio cumplimiento para todos los funcionarios, contratistas, o terceras personas que tengan acceso a los activos de información de Cenabastos S.A.

Todos los usuarios están obligados a continuar protegiendo la información y cumplir las políticas de seguridad de la información después de terminar su relación con la Sociedad.

Si un usuario viola las disposiciones de las políticas de seguridad de la información, por negligencia o intencionalmente, Cenabastos S.A., se reserva el derecho de aplicar las medidas pertinentes.

Entre otros se podrá solicitar el inicio de proceso disciplinario al funcionario o funcionarios que hayan violado las políticas y procedimientos de seguridad de la información.

Debido a la propia evolución de la tecnología, a las amenazas de seguridad y a las nuevas aportaciones legales en esta materia, Cenabastos S.A., se reserva el derecho a modificar estas políticas cuando sea necesario. Los cambios realizados en estas políticas serán divulgados a los usuarios y proveedores que les aplique, utilizando los medios que se consideren pertinentes, para garantizar la publicidad de los mismos.

DEBERES DE LOS FUNCIONARIOS Y CONTRATISTAS EN RELACIÓN CON LA INFORMACIÓN

Los funcionarios y contratistas de Cenabastos S.A., en relación con la información que se les entregue o a la que accedan para el desempeño de sus funciones o el cumplimiento de sus obligaciones contractuales, según el caso, así como los terceros usuarios de ella, tendrán los siguientes deberes:

• No revelar ni transmitir información reservada o sensible, sin la autorización previa y escrita, del dueño de la información.

• Custodiar el identificador de usuario y contraseña de cada sistema de información a su cargo y no revelarlos a persona alguna, bajo ningún concepto.

• Asumir toda actividad relacionada con el uso de su acceso autorizado.

• No utilizar ningún identificador y contraseña de otro usuario, aunque disponga de la autorización del propietario.

• Garantizar que el(los) equipo(s) quede(n) protegido(s) del acceso a personal no autorizado, cuando queden desatendidos (abandono temporal del activo de información).

• Tener acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones o el cumplimiento de sus obligaciones contractuales.