POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

BURICA .S.A

ABRIL 2017

COPIA 1

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La gestión de seguridad de la información implica la organización y coordinación de todos los esfuerzos encaminados al aseguramiento del entorno informático de la Entidad, para lo cual es necesario emplear mecanismos reguladores de las funciones y actividades desarrolladas por los funcionarios y terceros de la Compañía. La Política de Seguridad de la Información es la declaración general que representa la posición de la Dirección de **Burica S.A.** con respecto a la protección de los activos de información. En el presente documento se encuentra estructurado con una política general de seguridad de la información y políticas específicas que soportan el Sistema de Gestión de Seguridad de la Información, las cuales deben ser conocidas y aceptadas por todos los usuarios de la infraestructura tecnológica y la información de la compañía.

2. OBJETIVO

Dar a conocer a todos los funcionarios y terceros de La Compañía **Burica S.A.**, las políticas y estándares que se deben cumplir para proteger y/o preservar los activos informáticos y la información almacenada en ellos.

3. ALCANCE

Las políticas definidas en el presente manual aplican a todos los funcionarios y terceros de BURICA S.A. que utilicen recursos informáticos.

4. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% de las políticas.

5. SANCIONES POR INCUMPLIMIENTO

El incumplimiento del presente manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las Gerencias y/o las autoridades competentes.

6. REVISIÓN DE LA POLÍTICA

Las políticas de seguridad de la información del presente manual serán revisadas anualmente o cuando se identifiquen cambios en la estructura, objetivos o alguna condición que afecte la política, con el fin de asegurar que se encuentren ajustadas a los requerimientos de la Compañía **BURICA S.A.**

7. MARCO LEGAL

LEY 527 DE 1999

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

LEY 594 DE 2000

Por medio de la cual se dicta la ley general de archivos y se dictan otras disposiciones.

LEY 1266 DE 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1581 DE 2012

Por la cual se dictan disposiciones generales para la protección de datos personales.

LEY 1341 DE 2009

Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

LEY 1437 DE 2011

Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

LEY 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

LEY 1712 DE 2014

Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. NTC ISO/IEC 27001 DE 2005 Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la segundad de la información (SGSI), teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos. La norma adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA) para estructurar los procesos del SGSI.

8. ROLES Y RESPONSABILIDADES

La Dirección de Tecnología de información

a. Definir y establecer las políticas de seguridad de la información.
b. Coordinar la implementación de las políticas de seguridad de la información con los diferentes procesos de la Compañía Burica S.A.
c. Reportar a la Gerencia General, el estado de la seguridad de la información de la Entidad.

Gestion T.I.

El departamento de T.I deberá en forma activa implementar las medidas técnicas y procedimientos para brindar un nivel apropiado de seguridad de la información, de acuerdo a las políticas de seguridad de la información de la Compañía BURICA S.A.

Gestión Humana

Esta área se encargara de la revisión de requisitos para proceder a los diferentes cargos en La compañía BURICA S.A. Como parte de la función de selección se debe realizar una verificación de los antecedentes y referencias de los candidatos, garantizar que los funcionarios firmen el acuerdo de confidencialidad.

Gerencia General

Esta Área tiene como responsabilidad velar por el cumplimiento de las políticas definidas en la Compañía Burica S.A. y ejercer control sobre la gestión y actividades que adelanten las dependencias de acuerdo a lo definido en el Sistema de Control Interno. Los documentos y procedimientos relativos a la seguridad de la información los procesos y las cláusulas de confidencialidad de la información dentro de los contratos de los contratistas.

9. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

9.1. Política General

La Gerencia General, declara en la presente Política de Seguridad de la Información su posición y compromiso con respecto a la preservación de la confidencialidad, integridad y disponibilidad de sus activos de información (la información, los servicios, las tecnologías de información incluido el hardware y el software, las personas y la imagen de la Entidad), a la definición, implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información en el marco de la norma NTC ISO/IEC 27001 soportado en lineamientos claros alineados a las necesidades de la Entidad y a los requerimientos regulatorios, y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos, como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. Para lo cual establece las siguientes directrices:

- La identificación, clasificación y valoración de los activos de información de la Entidad, como base para la realización del análisis de los riesgos a los que están expuestos y así seleccionar e implementar los controles necesarios para reducir los riesgos a un nivel aceptable.

- El aseguramiento de las instalaciones físicas de la Entidad y las áreas de procesamiento de información, con el fin de evitar el acceso físico no autorizado, la interferencia o daño de la información propia o de terceros resguardada por la Entidad.

- El aseguramiento de la autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad, confidencialidad y conservación de los documentos físicos y electrónicos de archivo creados, procesados, transmitidos o resguardados por sus procesos con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta.

- En un plazo de seis (6) meses contados a partir de su aprobación, se hará la identificación y concertación de los requisitos para la seguridad de la información en la adquisición de nuevas aplicaciones, infraestructura y servicios.

- El aseguramiento, a través de una adecuada gestión, de los eventos de seguridad y las debilidades asociadas con los sistemas de información para una mejora efectiva de su modelo de seguridad.

- El suministro de recurso humano con la educación, formación y concientización en aspectos relacionados con seguridad de información necesaria y adecuada a las obligaciones y/o responsabilidades de los servidores públicos y/o terceros.

- El Establecimiento de roles y responsabilidades de los usuarios y/o terceros con el fin de crear compromisos en la protección de la información a la cual acceden y procesan, para evitar su pérdida, alteración, destrucción o uso indebido.

- El cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en materia de seguridad de la información. La presente política aplica para todos los funcionarios, terceros y proveedores que tengan acceso a los activos de información de la Entidad. Dicha política es de

obligatorio cumplimiento por parte de Funcionarios, terceros y proveedores; su falta de aplicación será sancionable conforme a las normas vigentes, dependiendo de su naturaleza y gravedad, dicha sanción será aplicada por las Gerencias y/o las autoridades competentes. Esta política será revisada anualmente o cuando se identifiquen cambios en la Compañía, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

- La aplicación de estas políticas son para las Gerencias, Jefes de área, administradores de puntos de ventas, asistentes, auxiliares, terceros, (contratistas, empleados temporales).

9.2. Política de Gestión de activos

- Los activos de información de la Compañía BURICA S.A., se identifican, clasifican y se valoran para establecer los mecanismos de protección necesarios, así mismo tendrán un propietario asociado quien es el responsable de definir quienes tienen acceso y que pueden hacer con la información.
- Los recursos TIC que no pertenezcan a la Compañía BURICA S.A., incluidos computadoras portátiles, teléfonos inteligentes, tabletas, etc. No deberán conectarse a las redes, a los sistemas ni a los servicios la Compañía (o utilizarse para obtener acceso a las aplicaciones de éste) sin la aprobación explícita del Departamento de T.I. y tras verificar que tales recursos cumplan con los requerimientos mínimos de seguridad de la Compañía (tales como software antivirus actualizado, cortafuegos habilitado, inexistencia de software de escaneo de redes u otros programas objetables). Lo anterior debido a que los dispositivos de comunicación personal (teléfonos inteligentes y tabletas) que se conecten a la red inalámbrica de la oficina, a los sistemas o a los servicios de la compañía que representan un riesgo para la seguridad de la información y una carga adicional a la conexión de Internet, ya que dichos dispositivos están normalmente conectados a cuentas personales de redes sociales u otros servicios.
- Todos los funcionarios y terceros que utilicen los recursos TIC deben seguir las políticas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, establecidos por la Compañía Burica S.A.
- Las medidas empleadas de protección para el cableado de la red y dispositivos de comunicación es que no se exhiban ni sean de fácil acceso generando el riesgo de conexiones no autorizadas.
- Se emplearan herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los equipos que contengan medios de almacenamiento y que serán reutilizados o eliminados, con el fin de garantizar que la información de la Entidad contenida en estos medios no se pueda recuperar.
- Los recursos de red que ha dispuesto por Burica S.A., tales como Directorios compartidos, Portal web, Intranet, Repositorio, etc., no deben ser utilizados para el almacenamiento de información que no es para propósitos laborales, ejemplos de información no permitida son: Material pornográfico, videos, películas, música, fotos, etc.
- Para adquisición de equipos de cómputo se tiene la opción de comprarlos a distintos proveedores o se toman a través del leasing corporativo con Fanalca S.A.
- Para la adquisición de Hardware se hacen dos cotizaciones y la gerencia General aprueba, luego de esto de procederá a realizar la orden de compra.

9.3. Política de Seguridad de los Recursos Humanos

- Todos los funcionarios y terceros (empleados temporales y contratistas) de la entidad deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la entidad, en cuanto a la seguridad informática y a la seguridad de la información según sea pertinente para sus funciones laborales.
    - Cuando se produzca una terminación de contrato, la oficina de gestión humana deberá informarlo de manera inmediata al Departamento de T.I. para el retiro de los accesos a la red y los sistemas de información.
    - Es responsabilidad de los funcionarios y terceros proteger los activos que estén bajo su custodia contra acceso, divulgación, modificación, destrucción o interferencia no autorizada, haciendo cumplir las medidas de seguridad implementadas por la Compañía.
    - Los funcionarios y terceros deben informar al Departamento de T.I los eventos detectados o potenciales u otros riesgos de seguridad para la Compañía.
    - Se debe resguardar la reserva de los documentos y bases de datos que contengan información personal de funcionarios y terceros que laboran durante y después de la terminación de los vínculos laborales con la Compañía.

9.4. Política de Acuerdos de Confidencialidad

- Todo funcionario de la Compañía Burica S.A. debe firmar en señal de aceptación el acuerdo de confidencialidad.
- Los Gerentes, Jefes y Administradores, deben ser responsables del acuerdo y deben velar porque las terceras partes cumplan las cláusulas de confidencialidad.
- Se deben ejecutar revisiones y auditorías en la prestación de servicios por terceros en cuanto al cumplimiento de las cláusulas de confidencialidad incluidas en los contratos.

9.5. Política de Acceso físico

- Se consideran áreas de acceso restringido a todas las áreas donde se encuentran alojados los equipos de procesamiento o almacenamiento de información privada, la infraestructura de soporte a los sistemas de información y comunicaciones, y las áreas donde se encuentran las bóvedas y bodegas donde se custodia el patrimonio documental y documentación privada; por lo cual se deben emplear mecanismos de acceso físico que garanticen que sólo se permite el acceso al personal autorizado.
- Las áreas de acceso restringido deberán siempre ser salvaguardadas y contar con mecanismos efectivos que permitan cumplir con los requerimientos ambientales de temperatura y humedad especificados por los fabricantes de los equipos que albergan, y conservación de la documentación que custodia, además de medidas para proteger los equipos del polvo y prevenir amenazas externas como manifestaciones sociales, explosiones en la calle o vandalismo.
- El acceso a las áreas restringidas por parte del personal de soporte técnico de proveedores se debe otorgar y monitorear, únicamente cuando sea necesario por medio de una autorización.
- Cuando sea viable, las áreas restringidas deben ser discretas y no tener indicaciones sobre su propósito, sin señales obvias que identifiquen las actividades de procesamiento de información o de la documentación que custodia.
- No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la entidad, a menos que esté autorizado.
- Todos los funcionarios y contratistas deben portar en un lugar visible el carnet que los identifica como funcionarios o contratistas de la Entidad para el acceso a la Entidad y mientras se encuentre dentro de ella.
- Todos los visitantes que ingresen a la Entidad deben ser registrados y deben portar una tarjeta que los identifique como visitantes en un lugar visible. Debe notificarse inmediatamente al personal de seguridad si se encuentran visitantes sin identificación visible.

9.6. Política de respaldo

- Se debe asegurar que la información contenida en la plataforma tecnológica de Burica S.A. como servidores, dispositivos de red para almacenamiento de información, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, confidencialidad, integridad y disponibilidad. El plan de restauración de copias de seguridad está dado por los lineamientos de FANALCA S.A. ya que toda la información de la base de datos, correos y nomina se encuentra en ese Datacenter esto con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.
- Los medios de almacenamiento que contienen la información de la copia de respaldo son de alta calidad y almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.
- Cada uno de los funcionarios y terceros que tengan bajo su responsabilidad la información necesaria para la ejecución de sus labores debe hacer copias de respaldo periódicas y almacenar la información de respaldo de manera segura pero accesible, con el fin de evitar su pérdida en caso de un incidente de seguridad, siguiendo los lineamientos del Departamento de T.I.
- Se realizará en cada punto de venta un backup de la base de datos de la tpv. Desatendida y se llevara una bitácora de la realización de este.

9.7. Política de
9.8. uso de internet

- El acceso al servicio de internet debe ser autorizado por el Departamento de T.I. quien vigilará su correcto uso y funcionamiento a través de herramientas de monitoreo y análisis de tráfico, dicho uso está priorizado exclusivamente para actividades institucionales.
- Los recursos TIC han de ser utilizados de manera responsable y entre las acciones no permitidas en el uso incluye el utilizar sistemas de intercambio de archivos (P2P, torrent, ares, Dropbox etc.) para obtener de manera ilegal material con derecho de autor, instalar software que no ha sido aprobado o utilizar los recursos TIC de la Entidad en violación de leyes de derecho de autor aplicables.
- El acceso a servicios de mensajería instantánea y redes sociales debe ser autorizado por la Gerencia General o por el Departamento de T.I.

Actividades Prohibidas

- Ingresar a páginas pornográficas así como de personas u organizaciones al margen de la ley o de contenidos ilegales.
- Descargar música y video, en especial con los servicios provistos por las páginas especializadas para tal fin, así como utilizar o participar en juegos de entretenimiento en línea.
- Utilizar los servicios de radio, videos y televisión a través de Internet, salvo que dicha información se requiera para el ejercicio de las funciones a cargo. En este caso el Jefe del Área o Dependencia correspondiente deberá mandar un correo, exponiendo las causas de la excepción ante el departamento de T.I.
- Descargar o instalar programas, modificar los paquetes y configuraciones ya instalados en los computadores de la Entidad.

9.9. Política de uso de correo electrónico institucional

- El servicio de correo electrónico institucional debe ser autorizado por el Departamento de T.I. y solo podrá ser utilizado para fines laborales, su configuración y acceso desde dispositivos móviles que no pertenezcan a la Entidad debe ser autorizado por la Gerencia General o el departamento de T.I. previa revisión de las medidas de seguridad mínimas que debe cumplir.
- Los administradores del sistema de correo electrónico emitirán cuentas de correo electrónico con el nombre de sus usuarios (funcionarios y terceros) asociadas al dominio BURICA.COM.CO, que utilizan la convención las iniciales del de los nombres y apellido (nnapellido@burica.com.co) para funcionarios y contratistas. Y en la firma de los mismos deberán incluir la dependencia al cual pertenece.
- No se permite el envío de correos con contenido que atente contra la integridad humana de las personas o instituciones, tales como: pornográfico, chistes, religiosos, terroristas, hackers, racistas, políticos o cualquier contenido que represente riesgo de virus; código malicioso, Rasonware (secuestro de información), etc.
- Sólo se permite el envío de correos masivos a los usuarios que lo requieran para el desarrollo de sus actividades laborales, previa autorización por parte del Departamento de T.I.
- No está permitido el envío de archivos adjuntos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- No es permitido en ningún caso accesar ni compartir mensajes de correos con información en archivos adjuntos de dudosa procedencia. Si se recibe un correo de origen desconocido, se debe consultar inmediatamente con el Departamento de T.I. sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos de correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keylogger, gusanos, etc.).
- Se deben eliminar permanentemente los mensajes innecesarios.
- La firma de los correos electrónicos será obligatoria tanto para funcionarios de planta como contratistas y deberá contener: Nombre y Apellidos, Cargo, Nombre Entidad, Teléfono de contacto y extensión. Ejemplo:

  Nombre
  Cargo
  Empresa o área a la que corresponde
  Teléfono y extensión
  Celular corporativo
  Dirección de la oficina
  Correo electrónico

- Los correos electrónicos deben contener la sentencia de confidencialidad con el siguiente contenido:

  CONFIDENCIALIDAD:

  Este mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley. Solo puede ser utilizada por la persona o compañía a la cual está dirigido. Si usted no es el receptor autorizado, o por error recibe este mensaje, favor borrarlo inmediatamente. Cualquier retención, difusión, distribución, copia o toma cualquier de acción basada en ella, se encuentra estrictamente prohibido.

- Corresponde a cada uno de los funcionarios y terceros dar el uso adecuado a estos recursos y en ningún momento podrán ser utilizados para realizar actividades ilícitas.

9.10. Política de control de acceso lógico

- Cada usuario es responsable de la cuenta de usuario y clave que le ha sido asignada necesaria para acceder a la información y a la infraestructura tecnológica de la Compañía. Los usuarios no deben divulgar ni permitir que otros utilicen sus cuentas de usuario, ni utilizar las cuentas de usuario de otros usuarios.
- Los Gerentes, Jefes de Área y Administradores de puntos deberán solicitar al Departamento de T.I. a través de la Gestion humana con el formato F-TI004 que la creación de los usuarios que requieran para el acceso a los sistemas de información y los servicios de red de la Entidad, para los cuales se establecerán privilegios de acceso de acuerdo a sus funciones y competencias.
- Los Gerentes, Jefes de oficina y administradores, deberán determinar los permisos y niveles de acceso a los documentos físicos y digitales que se le deberán otorgar a los usuarios de su área, teniendo en cuenta la clasificación de la información establecida en el inventario de activos de información.
- El acceso remoto a la red y a la infraestructura de procesamiento de información sólo podrá ser realizado por los usuarios autorizados por el Departamento de T.I. a través de la VPN siguiendo los requerimientos de seguridad determinados por éstos.
- El acceso a los sistemas de información y recursos TIC de la compañía BURICA S.A., será considerado un privilegio y no un derecho. Las cuentas de acceso se conceden específicamente con el fin de llevar a cabo las funciones de la compañía. Como tal, estas cuentas se mantendrán activas, siempre y cuando la persona a quien se asigna la cuenta siga llevando a cabo sus actividades.
- Cuando un funcionario o tercero se está separando o desvinculando de la compañía BURICA S.A., ya sea por destitución, retiro, jubilación o terminación del contrato, su/sus cuentas de acceso a los Sistemas de información y recursos TIC de BURICA S.A. incluida cuenta de correo electrónico) se suspenderá a partir de la fecha de separación o desvinculación y se eliminará a los 30 días siguientes, previa información y envió de correo electrónico por parte de parte de la Gestion Humana de BURICA S.A.
- Con carácter excepcional, una cuenta de acceso suspendida puede ser reactivada. La solicitud deberá hacerse por escrito al Departamento de T.I. precisando el motivo para activar la cuenta y el período de tiempo específico por el cual la cuenta se mantendrá activa. La solicitud debe venir directamente del jefe de Área o supervisor del contrato según corresponda.
- Las cuentas de acceso a los sistemas de información y a los recursos TIC de BURICA S.A. (incluyendo cuentas de correo electrónico), se suspenderán o cancelarán si no se registra actividad en estos sistemas por 180 días.
- Cada administrador de punto de venta en conjunto con la Gestion humana son responsables de crear incluir en los huelleros el personal previa lista enviada con los números libres, y luego informar mediante correo electrónico al departamento de T.I. para la inclusión en el software de reportes, Adjuntando la siguiente información (número de cedula, nombres, apellidos, dirección, teléfono, cargo).

9.11. Política de uso de software

- Los usuarios autorizados deberán solicitar la aprobación del Departamento de T.I. antes de instalar cualquier software que no haya sido aprobado previamente para su uso.
- No está permitida la distribución por cualquier medio, de software propiedad o con licencia de la Compañía BURICA S.A. a personal no autorizado.
- Para la adquisición de software en BURICA S.A. para server se requieren los lineamientos de Fanalca S.A. por temas de compatibilidad, clase de licenciamiento, estabilidad y demás, luego de evaluar estos temas se procede a pedir dos cotizaciones para la aprobación de la Gerencia General, para la realización de la orden de compra.
- Si el software es para maquinas locales, se evalúa la necesidad del usuario y se le brindan otras alternabas existentes, Si la alternativa no es suficiente para cubrir el requerimiento, se procede a pedir dos cotizaciones para aprobación de la Gerencia General, para la realización de la orden de compra.

9.12. Política de contraseñas

- Es responsabilidad de cada uno de los funcionarios y terceros que posean cuenta de usuario para el acceso a la red o los sistemas de información de la Compañía hacer buen uso de la misma, no divulgando ni escribiendo la contraseña en lugares visibles.
- La contraseña de la cuenta de usuario asignada por primera vez debe ser inmediatamente cambiada en el primer inicio de sesión, cumpliendo con los siguientes requisitos:
- Tener mínimo seis caracteres y 4 números: Caracteres en mayúsculas y minúsculas (es decir, Aa-Zz) Base de 4 dígitos (es decir, 0-9) y un carácter especial (es decir, !@#$%^&*()_+|~-= \ `{}[]:";'<>?,./).
- Se debe exigir el cambio de contraseña de red y del correo institucional cada 90 días, advirtiendo sobre éste cambio al usuario a partir de 5 días antes de su vencimiento.
- El grupo de sistemas no restablecerá contraseñas a un usuario, a menos que este mismo lo solicite y se identifique a sí mismo.
- Los usuarios no deben utilizar la misma contraseña de acceso a sus cuenta de acceso personal (cuenta de correo electrónico usuario@BURICA.COM.CO, Intranet, etc).
- El usuario debe evitar mantener un registro (por ejemplo, en papel, archivos electrónicos) de las contraseñas, a menos que se pueda almacenar de forma segura y el método de almacenamiento haya sido aprobado por el departamento de T.I
- Todo usuario autorizado debe cambiar las contraseñas cada vez que exista o haya algún indicio de una posible vulnerabilidad del sistema.

9.13. Política de protección contra software malicioso

• Se debe tener instalado como mínimo un software antivirus que brinde protección contra código malicioso en todos los recursos informáticos de la Entidad, asegurándose que estas herramientas no puedan ser deshabilitadas, así como de su actualización permanente.
• Cada uno de los funcionarios y terceros deben revisar previamente al acceso el dispositivo de almacenamiento removible con el antivirus. Cada uno es responsable por la seguridad física y lógica del dispositivo con el fin de no poner en riesgo la información de la Compañía BURICA.S.A.
• No está permitida la utilización de medios de almacenamiento virtual que no estén previamente autorizados por el Departamento de T.I.
• No está permitida la generación, propagación, ejecución o introducción de cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica de la Compañía.

9.14. Política de equipo desatendido

- Toda la información (documentos impresos, medios de almacenamiento removibles, cd´s) declarada no pública utilizada para el desarrollo de las actividades laborales, debe permanecer en lugares seguros o bajo llave en el escritorio mientras el puesto de trabajo esté desatendido o en horas no laborales con el fin de evitar pérdidas, alteraciones o accesos no autorizados. Adicionalmente.
- Toda la información no pública que se envía a las impresoras debe ser recogida de manera inmediata.
- Es responsabilidad de cada uno de los usuarios bloquear la sesión de su estación de trabajo mientras no se encuentre presente, la cual se podrá desbloquear sólo con la introducción de la contraseña del usuario. Al finalizar sus actividades del día, se deben cerrar todas las aplicaciones y apagar el equipo de cómputo.
- Es responsabilidad de cada administrador y segundos correr los procesos de sincronización de cada una de la Cajas desatendidas para que se realice respectiva actualización de precios y datos de clientes.

9.15. Política de intercambio de información.

- Todos los funcionarios y terceros que requieran conocer o intercambiar información no pública de la compañía, deberán firmar acuerdos de confidencialidad que será firmada por la Gerencia General de ambas partes, antes de obtener el acceso a la información, en los que quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes.
- Todos los funcionarios y terceros son responsables por la protección de la confidencialidad e integridad de la información y de los medios utilizados para el intercambio de información con el fin de no permitir una divulgación o modificación no autorizada.
- Es responsabilidad de los propietarios de la información que se requiere intercambiar, definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad requeridos.

9.16. Política de gestión de incidentes

• Los usuarios deben informar de cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los recursos TIC y/o la información al Departamento de T.I.

• seguir procedimientos para la gestión de los incidentes de seguridad de la información que permitan ejecutar de manera organizada las actividades de planificación, atención de incidentes y mejora continúa para enfrentar nuevos incidentes.

- Para eso se cuenta con plantas eléctricas.
- Se tiene contratado el servicio de datacenter con Fanalca.
- Se tiene contratado el 70% del servicio tecnológico con Fanalca.
- La gestión de incidentes con el ERP y POS se reporta con la casa desarrolladora SIESA, la cual nos brida soporte 24/7/365.
- Para los puntos propios se llaman contratistas para resolver nuestros impases, pero esto sin afectar las labores diarias.

10. GLOSARIO DE TERMINOS

Aceptación del riesgo: Decisión de asumir un riesgo.

Activo: Es todo aquello que tiene valor para la organización (Información, Software, Hardware, Servicios, Imagen institucional, Personas) y necesite protegerse.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Autenticidad: Permite verificar la identidad del generador de la información, evitando la suplantación de identidad.

Cifrado de datos: Es el proceso por el que una información legible se transforma mediante un algoritmo en información ilegible.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Conservación a largo plazo: Conjunto de acciones y estándares aplicados a los documentos durante su gestión para garantizar su preservación en el tiempo.

Contraseña: Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la Organización.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Documento electrónico de archivo: Registro de la información generada, recibida, almacenada, y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. Evento de seguridad de la información. Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Keylogger: Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet. Medios de almacenamiento removibles: comprende los discos duros externos, memorias USB, tarjetas SD, etc.

No repudio: el emisor no podrá negar el conocimiento de un mensaje de datos ni los compromisos adquiridos a partir de éste.

Política: Toda intención y directriz expresada formalmente por la Dirección. Riesgo. Combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad. Sistema de gestión de la seguridad de la información - SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar. Hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Sistema de gestión de documento electrónico de archivo – SGDEA: Sistema de gestión compuesto por elementos funcionales (sistema(s) de información o software especializado) y no funcionales (políticas, procesos y procedimientos) para la administración de documentos electrónicos de archivo, garantizando su autenticidad, fiabilidad, integridad y disponibilidad.
TIC: Las tecnologías de la información y la comunicación
Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Troyano: Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

Usuario: Toda persona, funcionario, que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

> **Usuarios Terceros:** Todas aquellas personas naturales o jurídicas, contratistas o temporales que no son funcionarios del la Compañía Burica S.A., pero que por las actividades que realizan en la Entidad, deban tener acceso a los recursos informáticos.

Virus: Programas, habitualmente ocultos dentro de otro programa, correo electrónico, pagina web, fichero o volumen. Se ejecutan automáticamente, haciendo copias de sí dentro de otros programas a los que infectan.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.