INDUSTRIA LICORERA DEL CAUCA

DO-GT-01

POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LA INDUSTRIA LICORERA DEL CAUCA

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Blanca Leticia Muñoz Muñoz JEFE DIVISIÓN PLANEACIÓN	Carolina Muñoz COORDINADOR DE CALIDAD	Julieta Ortiz Guerrero GERENTE
FECHA DE ELABORACION:	FECHA DE REVISION:	FECHA DE APROBACION:
28 de Marzo de 2022	30 de Marzo de 2022	01 de Abril de 2022

CONTENIDO

Contenido

INTRODUCCION 4

1. GENERALIDADES 4

1.1. SEGURIDAD EN LA EMPRESA 5

1.2. SEGURIDAD LÓGICA 5

1.3. SEGURIDAD FÍSICA 5

1.4. SEGURIDAD LEGAL 5

2. OBJETIVO 6

3. ALCANCE 6

4. TERMINOS Y DEFINICIONES 6

5. POLÍTICAS DE SEGURIDAD INFORMÁTICA 8

5.1. NIVEL DE SEGURIDAD EN LA EMPRESA 8

5.1.1. Políticas de seguridad 8

5.2. CLASIFICACIÓN Y CONTROL DE ACTIVOS 9

5.2.1. RESPONSABILIDAD POR LOS ACTIVOS 9

5.3. INVENTARIO DE ACTIVOS 9

5.4. RECOMENDACIONES USUARIOS FINALES 10

5.5. CLASIFICACIÓN DE LA INFORMACIÓN 10

5.6. SEGURIDAD LIGADA AL PERSONAL 11

5.7. CAPACITACIÓN DE USUARIOS 12

5.8. RESPUESTAS A INCIDENTES Y ANOMALÍAS DE SEGURIDAD 12

5.8.1. Copias de seguridad 12

5.8.2. Solicitudes de atención 13

5.9. NIVEL DE SEGURIDAD LÓGICO 13

5.9.1. Control de accesos 13

5.9.2. **Administración del acceso de usuarios** 14

5.9.3. **Responsabilidades del usuario** 14

5.9.4. **Uso de internet** 15

5.9.5. **Uso de correo electrónico** 15

5.10. **CONTROLES DE ACCESO INFORMÁTICO** 17

5.10.1. **Control de acceso a la red** 17

5.10.2. Control de acceso al sistema operativo 17
5.10.3. Control de acceso a servidores de la Industria Licorera Del Cauca 18
5.10.4. Control de acceso a las aplicaciones 18
5.11. GESTIÓN OPERACIONES Y COMUNICACIONES 19
5.11.1. Responsabilidades y procedimientos operativos 19
5.11.2. Adquisición y aceptación de aplicaciones y sistemas deinformación 19
5.11.3. Protección contra software malicioso 20
5.12. MANTENIMIENTO 21
5.13. MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO 21

6. **NIVEL DE SEGURIDAD FÍSICA** 21
6.1. SEGURIDAD FÍSICA Y AMBIENTAL 21
6.1.1. Seguridad de los equipos 21
6.1.2. Mantenimiento de equipos 22

7. **CONTROLES GENERALES** 23

8. **NOTIFICACION** 25

9. **APLICACIÓN Y CUMPLIMIENTO** 25

INTRODUCCION

La definición de políticas de seguridad Informática busca establecer en la Industria Licorera del Cauca una cultura de buenas prácticas que salvaguarden la seguridad de la información, sistemas de información y recursos tecnológicos de la empresa.

La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de Industria Licorera del Cauca en materia de seguridad.

Las políticas de seguridad informática establecen normas, reglas, procedimientos y controles que regulan la forma como la Industria Licorera del Cauca prevenga y maneje los riesgos de seguridad en diferentes circunstancias, el personal que utilice los servicios de la infraestructura tecnológica de laempresa deberá conocer y aceptar las políticas actuales sobre su uso, eldesconocimiento de las mismas no exonera de responsabilidad al usuario ante cualquier eventualidad que involucre la seguridad de la información o de la red de la empresa.

1. GENERALIDADES

En una empresa el área más susceptible a cambios es la de sistemas ya que esta área día a día nace, se adoptan y se implantan nuevas tecnologías razón por la cual se debe contar con una serie de políticas de seguridad que le permitan mantener los objetivos de la empresa.

En términos generales las políticas de seguridad informática, engloba los procedimientos más adecuados, tomando como lineamientos principales cuatro criterios, que se detallan a continuación:

1.1. SEGURIDAD EN LA EMPRESA

En la cual establece el marco formal de seguridad que debe sustentar laempresa, incluyendo servicios o contrataciones externas a la infraestructura tecnológica. Integrando el recurso humano con la tecnología, asignando responsabilidades y actividades complementarias como respuesta frente a situaciones que vulneren la seguridad de la infraestructura.

1.2. SEGURIDAD LÓGICA

Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre la gestión de soporte en sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

1.3. SEGURIDAD FÍSICA

Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

1.4. SEGURIDAD LEGAL

Integra los requerimientos de seguridad que deben cumplir todos los empleados y usuarios de la red la Industria Licorera del Cauca bajo la reglamentación interna de políticas y procedimientos de la empresa en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas

con la legislación del país y contrataciones externas.

2. OBJETIVO

Definir las políticas de seguridad con respecto al uso responsable de la infraestructura tecnológica de la Industria Licorera del Cauca.
Las políticas y procedimientos se han establecido con el fin de garantizar:

- La confidencialidad de la información
- La integridad de la información
- La disponibilidad de la información

3. ALCANCE

Estas políticas se aplicarán a todo el personal que tengan acceso al hardware, software, bases de datos, sistemas de información, intranet e internet, red datos, voz y potencia.

4. TERMINOS Y DEFINICIONES

- **Comunicaciones electrónicas:** usos de los sistemas de información para comunicar, publicar material y contenido por medios de servicios como correo electrónico, foros de discusión, paginas HTML o alguna herramienta similar.
- **Material no permitido:** Trasmisión, distribución o almacenamiento de todo material que viole cualquier ley aplicable, material protegido por derechos de reproducción, marca comercial u otro derecho sobre la propiedad intelectual utilizada sin debida autorización y material que resulte obsceno, difamatorio o ilegal bajo las leyes nacionales.
- **Intranet:** conjunto de recursos de conectividad computacionales que permiten la comunicación de datos e información a través de toda la empresa incluyendo el internet.
- **Internet:** Es una red de redes que permite la interconexión

descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP.

- **Redes:** incluye cualquier sistema cableado o equipos físicos como enrutadores, switches, sistemas electrónicos como redes de datos, voz, potencia y dispositivos de almacenamiento.
- **Sistemas de información:** sistemas o aplicaciones software que sea administrado por la empresa y de los cuales es responsable como Compromiso, Apoteosys, y Aurora, aplicaciones de servidores y escritorio.
- **Usuario:** Toda persona a quien se le proporcione los medios y niveles de autorización y acceso necesarios para hacer uso de los servicios o sistemas de información de la empresa.
- **Hardware:** Componentes tangibles que integran un equipo de cómputo.
- **Software:** Soporte lógico que permite que la computadora pueda desempeñar tareas inteligentes dirigiendo a los componentes físicos o hardware con instrucciones y datos a través de diferentes tipos de programas.
- **Bases de datos:** Sistema compuesto por un conjunto de datos organizados y que se relacionan entre sí y se almacenan en Discos que permiten acceso directo a la información.
- **Amenaza:** Es un evento o incidente en la empresa que pueda ocasionar daños materiales o perdidas inmateriales en los activos.
- **Ataque:** Evento que atenta sobre el buen funcionamiento de sistema.
- **Cuenta:** Mecanismo de identificación de un usuario dentro de un sistema informático.
- **Integridad:** proteger la información de posibles alteraciones y que pongan en riesgo la empresa.
- **Responsabilidad:** en términos de seguridad, significa que el personal de empresa es el responsable directo de mantener seguros los activos de cómputo e información.
- **Antivirus:** Programas que tienen como finalidad prevenir, bloquear, detectar y/o eliminar virus informáticos.
- **Virus Informático:** Programa ejecutable o pieza de código con habilidad

de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

5. POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las políticas de seguridad informática son creadas según el contexto de aplicación organizada por niveles de seguridad:

5.1. NIVEL DE SEGURIDAD EN LA EMPRESA

5.1.1. Políticas de seguridad

Los servicios de la red interna de la Industria Licorera de Cauca son de exclusivo uso del personal que aquí labora, la Gerencia y el comité de TICS delegará al proceso de Gestión Tecnológica para que dé seguimiento al cumplimiento de las políticas aquí establecidas el cual tendrá entre sus funciones:

a. Velar por la seguridad de los activos informáticos.
b. Gestión y procesamiento de información.
c. Hacer seguimiento al cumplimiento de las políticas de seguridad.
d. Elaboración de planes de contingencia y de seguridad.
e. Capacitación de usuarios en temas de seguridad.
f. Dar informes a la gerencia y al comité de TICS sobre problemas de seguridad.
g. Recibir de los usuarios de la infraestructura tecnológica sugerencias o quejas con respecto al funcionamiento de los activos y sistemas de información.

5.2. CLASIFICACIÓN Y CONTROL DE ACTIVOS

5.2.1. RESPONSABILIDAD POR LOS ACTIVOS

Todo personal al que se le asignen activos, según formato FOGT01 acta de entrega de activos informáticos, es el directo responsable de los activos asignados en su sitio de trabajo.

Nota: En caso de entregar un activo informático a un contratista a término fijo, el responsable del activo será su jefe inmediato.

5.3. INVENTARIO DE ACTIVOS

Los inventarios de activos permiten garantizar la protección eficaz de los recursos informáticos.

La Industria Licorera del Cauca debe identificar todos sus activos y el valor relativo e importancia de estos, sobre esta información se debe asignar niveles de protección a los activos. La oficina de gestión tecnologica identificará los activos informáticos y demás importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar y mantener un inventario con dicha información como aspecto importante para la administración de riesgos, este inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.
Cada activo debe ser claramente identificado, a quien está asignado clasificación respecto a seguridad y ubicación del activo.

5.4. RECOMENDACIONES USUARIOS FINALES

- No ingerir alimentos y bebidas en el área donde utilice el equipo de cómputo.
- No apagar el equipo, sin antes salir adecuadamente del sistema
- Hacer buen uso de los recursos de cómputo
- Realizar respaldos de información crítica periódicamente
- Consultar con el personal del área de soporte técnico cualquier duda o situación que se presente relacionada con los equipos informáticos.
- Cuidar las condiciones físicas de limpieza donde se encuentre el equipo
- Los usuarios NO pueden instalar ningún tipo de software en los equipos de propiedad de la Industria Licorera del Cauca, esta actividad es competencia únicamente del equipo de soporte técnico previa verificación de la existencia del licenciamiento.
- Está prohibido el uso de Medios de almacenamiento extraíble como USB y DISCOS EXTERNOS. Todos los dispositivos personales de información, computadores personales, asistentes digitales personales PDA, Celulares, no se pueden conectar a los equipos de la red de datos ni de potencia industria Licorera del Cauca.

5.5. CLASIFICACIÓN DE LA INFORMACIÓN

La información pública puede ser visualizada por cualquier persona dentro y fuera de empresa. La información interna es responsabilidad del personal y de la empresa, bajo ningún punto personas ajenas a un proceso podrán interveniro manipular la información, la información confidencial es propiedad absoluta dela Industria Licorera del Cauca. La información sensible que se debe proteger son:

- **Datos de interés para la competencia**: estrategias de marketing, listas de clientes, créditos con terceros, datos usados en decisiones de

inversión.

- **Datos que proveen acceso a la información o servicios**: llaves de encriptación o autenticación, contraseñas.
- **Datos del personal**: registros del personal, montos cartera clientes, datos históricos.
- **Datos que tienen alto riesgo de ser blanco de fraude u otra actividad ilícita:** datos contables utilizados en sistemas, sistemas que controlan desembolsos de fondos.
- **Aplicación de controles para la información clasificada:** el ambiente donde se almacena la información clasificada como “Restringida”, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado.

Los usuarios que utilizan documentos con información confidencial o restringida deben asegurarse de:

- Almacenarlos en lugares adecuados
- Evitar que usuarios no autorizados accedan a dichos documentos

5.6. SEGURIDAD LIGADA AL PERSONAL

En relación con los contratos**,** todo el personal que ejerza labores en la Industria Licorera del Cauca, no tiene ningún derecho sobre la información que procese dentro la empresa, en la red de datos de la empresa, en los sistemas de información y bases de datos.

La información que maneje el personal no puede ser divulgada a terceros ni por fuera de la empresa.

Los usuarios o personal encargado de activos informáticos es el responsable de las acciones causadas por sus operaciones en el equipo y en la red de la empresa y se rigen por las políticas de seguridad informáticas.

El responsable del área de Talento Humano incluirá las obligaciones relativas a la seguridad de la información y del área de trabajo en los respectivos contratos, informara a todo el personal que ingresa respecto al cumplimiento de las políticas de Seguridad de la Industria Licorera Del Cauca.

La Sección de Talento humano debe notificar a la oficina de sistemas la renuncia o despido de los empleados, así como el inicio y fin de los periodos de vacacionesde los mismos, con el fin de hacer un respaldo de la información, y mantenimiento correctivo y preventivo.

5.7. CAPACITACIÓN DE USUARIOS

La oficina de sistemas es responsable de promover constantemente la importancia de la seguridad a todos los usuarios de la infraestructura tecnológica de la Industria Licorera del Cauca.
El programa de concientización y cultura en seguridad informática debe contener continuas capacitaciones, charlas, adicionalmente se pueden emplear diversos métodos como afiches, mensajes a través de correo en los cuales se recuerde permanentemente al usuario el papel importante que cumple el cumplimiento de las políticas de seguridad.
Cuando ingrese personal nuevo a la empresa se debe entregar la política de seguridad, así como los procedimientos para el uso de los recursos, aplicacionesy sistemas de información.

5.8. RESPUESTAS A INCIDENTES Y ANOMALÍAS DE SEGURIDAD

5.8.1. Copias de seguridad

La empresa debe contar con respaldos de seguridad de la información dentro y por fuera de la empresa, ante cualquier riesgo o evento que se presente, generar procedimientos para protección de los datos.

5.8.2. Solicitudes de atención

El personal encargado de la administración de seguridad debe ser plenamente identificado por todo el personal que labora en la Industria Licorera del Cauca, en situaciones de emergencia que impliquen atención a los usuarios se debe dar prioridad según nivel jerárquico de la empresa.

Si el personal detecta o sospecha de la ocurrencia de un incidente de seguridad debe notificarlo al personal de sistemas, si se sospecha de la presencia de un virus en un sistema el usuario debe desconectar el equipo de la red de datos mientras llega el personal de sistemas a tender la solicitud.

La oficina de sistemas debe documentar todos reportes de incidentes de los usuarios.

5.9. NIVEL DE SEGURIDAD LÓGICO

5.9.1. Control de accesos

La información manejada por los sistemas de información y las redes asociadas debe estar adecuadamente protegida contra modificaciones no autorizadas, divulgación o destrucción. La oficina de sistemas proporcionara la información necesaria (manuales, procedimientos, formatos, políticas de seguridad informática) para el manejo de los activos informáticos, esto con el fin de cumplir con los siguientes objetivos:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y sistemas de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la empresa y otras redes públicas y privadas.
- Registrar y revisar eventos y actividades criticas llevadas a cabo por los usuarios en los sistemas.

5.9.2. Administración del acceso de usuarios

Son usuarios de la red de la empresa todo el personal administrativo, secretarias, contratistas y toda aquella persona que tenga asignados y que utilice los activos informáticos.

Se asignaran cuentas de usuarios únicas de acceso a los sistemas de información de la intranet al personal que lo requiera según el cargo y funciones que ejerza. Cada usuario de los sistemas de información debe ser identificado de manera única, y el acceso del usuario así como su actividad en los sistemas debe ser controlado, monitoreado y revisado

Cada cuenta de usuario debe tener una contraseña segura la longitud mínima de caracteres permitidos se estable en ocho caracteres, máximo diez caracteres, estos deben ser alfa numéricos, debe contener por lo menos una letra en mayúscula, un número y un carácter especial. Las contraseñas deben ser difícil de descifrar, no utilizar secuencias comunes de caracteres como por ejemplo 123456, detalles personales como fechas de cumpleaños, nombres de familiares, numero de documento de identidad, número de teléfono u otros que tengan relación directa con el usuario.

El acceso no autorizado a los sistemas de información puede generar sanciones disciplinarias.

5.9.3. Responsabilidades del usuario

El usuario es el responsable directo de su contraseña, del uso que haga de los sistemas de información con su cuenta y de la información que procesa, so pena de incurrir en un proceso disciplinario por mal uso de los servicios informáticos de la empresa.

El usuario debe evitar escribir las contraseñas en papel, superficies o dejar constancia de ellas, debe evitar que las contraseñas tengan relación con datos personales, nombres, fechas especiales o algún otro dato importante.

El usuario debe proteger su equipo utilizando contraseñas para el ingreso al sistema operativo, evitando que personas ajenas a su cargo puedan acceder a la información del equipo.

Cualquier usuario que encuentre una falla o hueco de seguridad debe reportarlo a la oficina de sistemas.

5.9.4. Uso de internet

El acceso a Internet provisto al personal de la Industria Licorera del Cauca es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

El acceso a internet tiene que ser realizado a través de los canales de acceso provistos por la Empresa, los usuarios de navegación en internet están sujetos de monitoreo de las actividades que realizan en internet.

5.9.5. Uso de correo electrónico

El servicio de correo electrónico está contratado con Google y se debe utilizar teniendo en cuenta todas las disposiciones de seguridad, la cuentas de correo deben ser con relación a las actividades de la empresa por lo tanto no deben haber correos personales debido a la capacidad de almacenamiento y por seguridad de la información de la empresa, se debe evitar el uso personal ya que en este tipo de correos se expone al envió de fotos, videos y demás archivos que ocupan gran espacio y además pueden ser nocivos para el equipo por los virus informáticos.

El correo electrónico es de uso exclusivo para el personal de la Industria Licorera del Cauca, el usuario será responsable de la información que sea enviada y recibida desde su cuenta.

- Los Usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado a nuestra Empresa.
- Es una falta grave facilitar y ofrecer su cuenta de correo electrónico (e-mail) a personas no autorizadas, su cuenta es personal e intransferible.
- El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión de información.
- La violación de la seguridad de los sistemas de nuestra red, pueden incurrir en responsabilidades civiles y penales.
- No es correcto enviar correo a personas que no desean recibirlo. Si la Empresa recibe quejas, denuncias o reclamaciones por estas prácticas, se cancelará su cuenta.
- Están completamente prohibidas las siguientes actividades:

  - Utilizar el Correo Electrónico para cualquier propósito comercial o financiero.
  - No se debe participar en la propagación de “cartas en cadenas”, ni en esquemas piramidales de índole político, religioso o temas similares.
  - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra Institución.

- Debido a que el espacio de las cuentas incide directamente sobre el espacio del servidor, se establecen que:

  - Todos los Usuarios deben de revisar frecuentemente su Correo Electrónico para leer sus mensajes, de modo que generen copia si los necesitan o los vayan borrando para no afectar el espacio de almacenamiento en el servidor.

5.10. CONTROLES DE ACCESO INFORMÁTICO

5.10.1. Control de acceso a la red

El acceso a la red interna se permitirá siempre y cuando el personal conozca los requisitos mínimos de seguridad, se debe eliminar cualquier acceso a la red por usuarios no identificados en la red.

La oficina de sistemas es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, es responsable de difundir las políticas de seguridad para el uso de la red y procurar su cumplimiento.

La oficina de sistemas deberá emplear herramientas para el bloqueo, enrutamiento, filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

Todas las conexiones entre la red interna de la empresa e internet deben ser controladas por un Firewall para prevenir accesos no autorizados.

Todos los componentes de la red de datos deben ser identificados de manera única y su uso restringido, esto incluye la protección física de todos los puntos vulnerables de la red.

Todos los dispositivos de la red, así como el cableado deben ser ubicados de manera segura

5.10.2. Control de acceso al sistema operativo

Al terminar una sesión de trabajo en el equipo evitar dejarlo encendido para prevenir la utilización del equipo por otras personas.

En ausencia no dejar activos los aplicativos como Apoteosys, Sevenet o

aurora, esto puede generar que otra persona manipule la información de su cuenta.

La oficina de sistemas debe establecer privilegios a los usuarios de acuerdo con sus necesidades, controlar que solo exista software permitido y con licencias de la empresa.

5.10.3. Control de acceso a servidores de la Industria Licorera Del Cauca

Es responsabilidad del personal de sistemas, toda aplicación instalada en los servidores será ejecutado bajo las cuentas de usuario requeridas para el ingreso a las aplicaciones o sistemas de información.

El acceso lógico a los servidores, enrutadores, bases de datos, conectados a la red es administrado por la oficina de sistemas.

5.10.4. Control de acceso a las aplicaciones

Las aplicaciones deberán estar correctamente diseñadas, con funciones específicas para cada usuario de la aplicación, el perfil del usuario debe estar habilitado en el sistema.

Se debe otorgar a los usuarios acceso solamente a la información necesaria para la realización de sus labores.

Se deberá hacer seguimiento de las aplicaciones sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, equipo desde donde conecta, de tal forma que se proporcione información relevante y revisable posteriormente.

5.11. GESTIÓN OPERACIONES Y COMUNICACIONES

5.11.1. Responsabilidades y procedimientos operativos

La oficina de sistemas es el responsable de la configuración y puesta en marcha de los sistemas y aplicaciones. El personal responsable de cada proceso llevara registros de fallas de seguridad del sistema, de igual forma hacer conocer las fallas al personal de sistemas.

Todos los sistemas de información y aplicaciones que utilice la Industria Licorera del cauca deberán estar legalmente registrado y con los respectivos contratos de soporte de Software y con sus respectivas licencias vigentes

Establecer y controlar, restringiendo si es necesario, el uso de dispositivos personales, tales como discos externos o memorias USB, entre otros, por parte del personal.

Bloquear determinados hardware, mediante sistemas de reconocimiento de usuario; o utilizar softwares que permitan saber si hay algún empleado que se esté tratando de filtrar información a través de medios como el email o tecnologías como Skype, redes sociales, por ejemplo.

5.11.2. Adquisición y aceptación de aplicaciones y sistemas de información

La oficina de sistemas será la encargada de realizar el proceso de planificación, desarrollo, adquisición, comparación, adaptación, del software necesario para la empresa.

La aceptación del software se hará efectiva por el comité de Tics y la Gerencia previo análisis y pruebas realizadas por el personal de sistemas de la empresa

Las pruebas de las aplicaciones o sistemas se deberán hacer teniendo en cuenta las medidas de protección de los datos, estas pruebas deben ser documentadas.

Es responsabilidad de la oficina de sistemas la realización de pruebas de validación de entradas en cuanto a:

a) Valores fuera de rango.
b) Caracteres inválidos, en los campos de datos.
c) Datos incompletos.
d) Datos con longitud excedente o valor fuera de rango.
e) Datos no autorizados o inconsistentes.
f) Procedimientos operativos de validación de errores
g) Procedimientos operativos para validación de caracteres.
h) Procedimientos operativos para validación de la integridad de los datos.
i) Procedimientos operativos para validación e integridad de las salidas.

5.11.3. Protección contra software malicioso

Se debe adquirir y utilizar software únicamente de fuentes confiables, los servidores al igual que los equipos de trabajo deben estar con el software antivirus debidamente instalado, configurado y tener activada la protección en tiempo real.

El personal de la Industria Licorera del Cauca no podrá bajar o descargar software de sistemas, correos electrónicos personales, mensajería instantánea, redes sociales y de comunicación externa. En caso de que se requiera la utilización de estos servicios debe contar con la autorización de la oficina de sistemas.

Cualquier usuario que sospeche de alguna infección por virus deberá dejar de usar el equipo y notificar al personal de sistemas.

5.12. MANTENIMIENTO

El mantenimiento de los sistemas de información y aplicaciones es responsabilidad del personal de sistemas. El cambio de archivos del sistema no es permitido si una justificación aceptable y verificada por el personal de sistemas.

Se debe realizar un registro del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

El usuario debe asegurarse de sacar copias de seguridad o respaldo de la información que consideré relevante cuando el equipo se envié a reparación.

5.13. MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

Las copias de seguridad se deben realizar según procedimiento de copias de seguridad, los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados únicamente por el personal de sistemas.

6. NIVEL DE SEGURIDAD FÍSICA

6.1. SEGURIDAD FÍSICA Y AMBIENTAL

6.1.1. Seguridad de los equipos

Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirara sellos de los mismos sin la autorización de la oficina de sistemas. Los activos informáticos estarán asignados al personal encargado de su conservación y manejo en la ubicación autorizada.

Los activos informáticos asignados serán de uso exclusivo para las funciones del personal de la Industria Licorera del Cauca a quien se le asigna el activo.

Es responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas ofimáticas y sistema operativo a fin de evitar riesgos por mal manejo y aprovechar al máximo las herramientas.

Es responsabilidad del usuario almacenar la información en una partición de la unidad de almacenamiento diferente al C:\ que está destinada para los archivos de programa y sistemas operativos

Mientras se esté operando en el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

Se debe evitar colocar objetos sobre el equipo de cómputo o tapar las salidas de ventilaciones monitor o de la torre se debe mantener el equipo informático en un lugar limpio y sin humedad.

El usuario responsable del activo debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar la reubicación de cables a la oficina de sistemas.

En caso de requerir cambios múltiples de los equipos de cómputo derivado de la reubicación de lugares físicos de trabajo o cambio locativos, estos deberán ser notificados con al menos cinco días de anticipación a la oficina de sistemas.

6.1.2. Mantenimiento de equipos

Se realizará mantenimiento de los equipos de cómputo para asegurar su disponibilidad e integridad permanentes, teniendo en cuenta a tal efecto:

Realizar tareas Soporte y Mantenimiento de Equipos según procedimientos establecidos en el proceso de Gestión Tecnológica para las tareas de mantenimiento preventivo, se realizarán de acuerdo con los intervalos de servicio y especificaciones recomendadas por el proveedor y con la autorización formal del responsable del área de sistemas.

Está prohibido que el usuario o personal diferente al personal de sistemas abra o destape los equipos de cómputo.

El usuario es responsable de comunicar a la oficina de sistemas la perdida de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

Los servidores deberán ubicarse en un área aislada y protegida estos serán manejados solo por el personal de sistemas

7. CONTROLES GENERALES

En ningún momento se debe dejar información sensible o expuesta al robo, manipulación, o acceso visual de los activos informáticos que manejan información crítica de la empresa esta información no puede ser alcanzada por terceros o personas que no deban tener acceso a esta.

Deberá llevarse un control, exhaustivo de mantenimiento preventivo y correctivo que se haga sobre los equipos.

Las áreas de trabajo deben contar con extintores necesarios para salvaguardar los activos informáticos.
El cuarto de telecomunicaciones debe estar separado de las demás áreas de la empresa.

El suministro de energía eléctrica debe hacerse a través de un circuito regulado y conectado a UPS.

Actualice regularmente su sistema operativo y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web. A veces, los sistemas operativos presentan fallos, que pueden ser aprovechados por delincuentes informáticos. Frecuentemente aparecen actualizaciones que solucionan dichos fallos. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, le ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

Instalar un Antivirus y actualizar con frecuencia. Analizar con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.
Instalar un Firewall o Cortafuegos con el fin de restringir accesos no autorizados de Internet.

Es recomendable incluir en la instalación de los equipos algún tipo de software anti- spyware, para evitar que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario.
Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la Oficina de Sistemas.

Ningún usuario de la red de la Industria Licorera del Cauca, debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por la Oficina de Sistemas.
No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de la Industria Licorera del Cauca.

8. NOTIFICACION

Con el fin de dar a conocer y socializar las políticas de seguridad informática la oficina de sistemas convocara al comité de Tics para la aprobación de las políticas y posterior socialización y capacitación con todo el personal de la Industria Licorera del Cauca, dejando evidencias físicas

9. APLICACIÓN Y CUMPLIMIENTO

Las políticas de seguridad informática aplican a todo el personal de la Industria Licorera del Cauca, cualquier usuario que viola las políticas aquí establecidas será objeto de sanción disciplinaria.

Proyectó:
Jhon Jaime Martínez Alegría
Técnico Programador De Sistemas