empresa para la seguridad urbana

EMPRESA PARA LA SEGURIDAD URBANA
ESU

Circular 003
(10 de Marzo de 2011)

DE: Gerente

PARA: Personal de la ESU

ASUNTO: Políticas de Seguridad Informática

Para garantizar la protección de la información, la plataforma informática y los sistemas de información de la Entidad, sírvanse encontrar adjunto, el documento "POLÍTICAS DE SEGURIDAD INFORMÁTICA", cuyo contenido es de obligatorio cumplimiento para todos los servidores de la Empresa para la Seguridad Urbana ESU.

JESÚS MARÍA RAMÍREZ CANO
Gerente

## 1. INTRODUCCION

La necesidad de contar con directrices que orienten el uso adecuado de las herramientas informáticas, obteniendo así el mayor beneficio y evitando el uso indebido de las mismas; las políticas de seguridad informática son una herramienta administrativa muy poderosa, diseñada para concientizar a los usuarios que utilizan dispositivos informáticos sobre la importancia de la información en las instituciones.

Para garantizar la seguridad de los datos en la plataforma informática se debe contar con barreras efectivas de protección tales como antivirus, filtros de contenido, control de correo Spam, protocolos de recuperación de datos, protocolos de acceso a la red, entre otros; necesarios para ofrecer una información confiable como soporte para la toma de decisiones;

## 2. PROPÓSITO DE LAS POLITICAS DE SEGURIDAD

Implementar las políticas de seguridad de la plataforma informática, como base para ofrecer una información veraz y confiable, fundamental para la correcta toma de decisiones, garantizando con estas la conservación y custodia de los datos como uno de los activos más importantes de la organización.

## 3. OBJETIVOS DE LAS POLITICAS DE SEGURIDAD

- Garantizar la salvaguarda y custodia de la información
- Implementar protocolos de manejo y generación de la información en la plataforma informática
- Informar los deberes de los usuarios con en el manejo de la información

## 4. HARDWARE Y SOFTWARE DE LA PLATAFORMA INFORMATICA

- El uso de los equipos es única y exclusivamente para dar cumplimiento a las tareas asignadas a cada funcionario.
- La instalación de cualquier programa debe ser realizada por el Profesional Administrador de la Red o previa certificación de éste.
- Se realizaran chequeos permanentes para verificar que no existan copias ilegales.
- Para realizar cualquier traslado o retirar un equipo se debe contar con la debida autorización del Profesional Administrador de la Red y el Profesional de Inventarios.
- Para dar de baja un equipo, su disco duro deberá ser borrado y formateado.
- Se restringirán los permisos a los usuarios para evitar descargas de programas ilegales.
- Se restringirá el acceso a las memorias USB a los equipos que no lo necesiten.
- Se deben utilizar contraseñas seguras compuestas por números, letras mayúsculas y minúsculas, para el ingreso a la red y a los aplicativos, Estas no deben verse al momento de ser digitadas.

- El mantenimiento preventivo de la plataforma informática se debe hacer por lo menos dos veces al año, tanto en los servidores como en los equipos de escritorio y dispositivos agregados a la red.
- Todos los equipos de la plataforma informática deben estar sincronizados con la fecha y hora de la controladora de dominio (servidor Godtrust) en concordancia con el reloj atómico de la entidad.
- Todo dispositivo de la plataforma informática debe estar asegurados.
- Se implementarán barreras de protección en la plataforma informática como antivirus, filtros de contenido, control de correo Spam, protocolos de recuperación de datos, protocolos de acceso a la red, protocolos de actualización, entre otros para garantizar la salvaguarda y custodia de la información
- Se harán capacitaciones y actualizaciones a los usuarios de la plataforma informática sobre manejo de los equipos y los aplicativos implementados en la entidad.

## 5. RESPONSABILIDAD DEL PERSONAL DE SISTEMAS

- El Profesional Administrador de la Red es el responsable de la instalación de todos los programas y equipos de la organización.
- Se harán auditorias semestrales para identificar la vulnerabilidad de la plataforma informática.
- Se harán evaluaciones semestrales a la red eléctrica regulada, a la UPC, los toma corrientes y los cables para evitar fallas que perjudiquen la plataforma informática.
- Se harán evaluaciones semestrales a la red de datos para evitar fallas que perjudiquen la plataforma informática.
- Se realizara un inventario anual de los dispositivos electrónicos de la plataforma informática.
- Todos los equipos de la plataforma informática estarán en buen estado, los usuarios contarán con herramientas informáticas suficientes para desempeñar su labor diaria y se le darán los privilegios de acceso según su perfil.

## 6. DERECHOS Y RESPONSABILIDADES DE LA ESU

- La ESU se reserva todos los derechos sobre la información y los datos generados en su plataforma informática. Los usuarios de la plataforma informática no tienen derecho a más privacidad que la que les otorga la ley para actividades sindicales
- La ESU se reserva todos los derechos de propiedad intelectual de cualquier material, aun en caso de que estos sean publicados en un foro público. El uso y divulgación de cualquier material deberá ser autorizado por la Secretaria Jurídica.
- Todas las memorias USB deben ser vacunadas antes de ser utilizadas en la plataforma informática.
- Se prohíbe el manejo de la información en equipos ajenos a la plataforma informática.

- Se prohíbe el consumo de alimentos y bebidas cerca de los dispositivos informáticos, cualquier daño en alguno de estos por esta causa será cargado a la persona responsable.
- Toda la información ingresada al sistema de información debe ser veraz y confiable.
- En caso de fugas de información se informara inmediatamente al Gerente Administrativo para tomar las acciones pertinentes.
- Se prohíbe enviar correos que no tengan que ver con las tareas funcionario y enviar correos de cadena.
- Se prohíbe el uso de correos diferentes al institucional, tales como Hotmail, Gmail, Latinmail, entre otros.

## 7. CONFIDENCIALIDAD DE LA INFORMACIÓN

- La información generada en la plataforma informática será considerada como confidencial y es responsabilidad de cada funcionario protegerla; debe evitarse el envío de esta por fuera de la plataforma informática, si por algún motivo esta es enviada, se debe solicitar la confidencialidad al receptor.
- Toda la información será almacenada en los servidores de la plataforma informática; el acceso físico a la dicha zona es exclusivo para personal autorizado.
- Toda persona al firmar su contrato con la ESU debe llenar un compromiso de confidencialidad de la información.
- Toda persona al retirarse de la ESU debe llenar un compromiso de confidencialidad de la información.
- En caso de retirar un funcionario de la ESU se deben suspender su buzón de correo y sus credenciales.
- Se harán copias de seguridad diariamente en cinta a la información critica de la plataforma informática, y se capacitara a los usuarios en la forma de realizar respaldo de su información; esta estará almacenada en la unidad D:\ de cada equipo asignado y es responsabilidad solo del funcionario.
- El antivirus se debe actualizar automática y permanentemente desde la consola de servicios.

Espero la colaboración de cada uno de ustedes para el logro de nuestros objetivos comunes.

Cordialmente,

Profesional Administrador de la Red

Vo.Bo. Director Administrativo y Financiero