POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Generales de la Información

La Política de Seguridad de Información son aquellos planes y acciones definidos e implementados a fin de garantizar la preservación y mantenimiento de toda aquella información procesada y efectuada por el personal de todas las áreas de la entidad, esta información pasara a ser propiedad intelectual y física del “IDUVI”

Por lo cual la política de seguridad de la Información pretende:

1. Velar por integridad, confidencialidad y la disponibilidad de la información que se genera en la entidad.
2. Se generarán copias de seguridad externas de los sistemas de información bases de datos, implementados por la entidad por parte del área de sistemas.
3. Los funcionarios de la entidad tendrán acceso a información según su área y funciones del cargo.
4. Los funcionarios no podrán distribuir o suministrar datos o información confidencial de la entidad.
5. Los funcionarios y contratistas de la entidad tendran confidencialidad de la información que se genere.
6. El funcionario o contratista de la entidad que intente violar o vulnerar la seguridad de los sistemas de información o servidores será sujeto a acciones legales.
7. La entidad se reserva el derecho a restringir el acceso a cualquier información en el momento que lo considere.
8. La información almacenada en el correo electrónico es de carácter personal, y se rige basado en términos y condiciones al momento de la asignación.
9. Todos los usuarios con acceso a un sistema de información o a la red informática de la entidad dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña, serán responsables de las acciones realizadas por el usuario que ha sido asignado.
10. Todos los usuarios de la entidad, deben reportar los incidentes de seguridad que se presenten, según el procedimiento de gestión de incidentes vigente en la entidad.

Disposiciones Específicas

1. Toda información guardada, contará con un directorio en un medio de almacenamiento independiente que permita conocer todas las características y facilite la plena identificación de la información respaldada.
2. El IDUVI, dispondrá de un sistema de respaldo de información para minimizar los daños y proteger la información procesada, al nivel de base de datos, aplicaciones, configuración de los sistemas operativos y de comunicaciones.
3. Los funcionarios de cada una de las dependencias de la entidad, que tienen asignado un equipo de cómputo son responsables de la organización de su propia información local, para facilitar su respaldo.
4. El funcionario a cargo, verificará que los equipos donde se graba la información reciban mantenimiento preventivo y correctivo.
5. La información almacenada se mantendrá por un período que estime conveniente la entidad, en concordancia con las normas y directivas emitidas sobre ese aspecto, así como de las necesidades funcionales y administrativas que reporte.

7. PROHIBICIONES ESTABLECIDAS Las prohibiciones que a continuación se detallan, describen las conductas indebidas:

1. Alterar los sistemas y configuración del equipo informático sin autorización área de Gestión TICS.
2. Intervenir o modificar la estructura de red eléctrica.
3. Extraer archivos o información consignada como propiedad física o intelectual del IDUVI, sin el previo conocimiento de los responsables de cada área usuaria, lo cual será comunicado al gerente, para su conocimiento y fines pertinentes.
4. La extracción de los ambientes de almacenamiento de las áreas asignadas para la seguridad de la información, de documentación, sin la previa autorización y en el caso del uso de esta para fines diferentes a los establecidos, y/o de cualquier índole personal, se tomaran las medidas legales correspondientes.
5. La modificación de ubicación y de acceso de uso o de configuración de IP, diferentes funcionarios sin la previa autorización.
6. Acceder a la información, cuentas, archivos o correo electrónico de otros funcionarios sin su autorización previa, preciando que esto constituye una violación tanto a la propiedad intelectual y física, en los casos de la

información procesada por el funcionario, así como en el caso de documentos de índole personal.

7. Instalar, copiar, distribuir o usar programas en violación a las leyes y/o reglamentos internos del IDUVI.
8. Usar el equipo de cómputo para fines particulares, excepto en la situación en las cuales el establecer alguna coordinación de tipo personal (revisión de e-mail, revisión de agendas personales), lo cual tenga un nivel de vinculación con las acciones laborales correspondientes a su funciones.
9. Abrir los equipos de cómputo sin autorización, así como cambiar las piezas.
10. Instalar Software innecesario, en este caso aquellos programas que no son de utilidad para el uso laboral del área usuaria.

8. USO DE INTERNET

1. El acceso a Internet y a los servicios asociados que proporciona la entidad deberán utilizarse para los propósitos de la propia entidad, de acuerdo con las atribuciones y funciones laborales del funcionario, establecidas en el manual de procedimientos.
2. Cuando el funcionario haga uso del servicio de Internet, deberá mantener un comportamiento de acuerdo con los principios éticos establecidos en el Código de Ética y Buen Gobierno, esto es, abstenerse de realizar cualquier actividad que a continuación se describe: - Realizar cualquier actividad intencional que provoque problemas con el funcionamiento de las redes, con otros usuarios, canales de comunicación, sistemas y equipos, como por ejemplo, propagar un virus informático. - Compartir o divulgar números de cuenta, claves de acceso y número de identificación personal u otra información confidencial o sensible para la entidad o que viole la Ley de Transparencia y Acceso a la Información Pública. - Obtener de Internet cualquier material en contravención la ley de derechos de autor. - Visitar en horarios laborables sitios que no tengan relación con las funciones de su trabajo, así como consultar, enviar, propagar o promover material o sitios que vayan contra la moral y las buenas costumbres, o que constituya o fomente un comportamiento que de lugar a responsabilidades civiles, administrativas

o penales. - Visitar sitios de chat, que no tengan relación con actividades propias de la entidad.

3. El funcionario deberá verificar que los archivos obtenidos de internet no contengan ningún virus informático que ponga en riesgo los bienes de la entidad.
4. El funcionario a cargo se encuentra facultado para bloquear todos aquellos sitios de internet que considere que no son compatibles con las labores de los funcionarios.

9. CORREO ELECTRONICO

1. El correo electrónico deberá ser usado exclusivamente para los propósitos de la entidad.
2. El funcionario es responsable de la información enviada o reenviada desde su buzón de correo electrónico.
3. El usuario de este servicio deberá mantener una imagen y comportamiento profesional cuando haga uso del correo electrónico, deberá abstenerse de realizar cualquiera de las actividades que a continuación se describen: a) Enviar correos masivos a todo el personal de la entidad. Cuando se requiera, el contenido será tratado como información a publicar en los sitios Web del IDUVI. b) Enviar cadenas de mensajes a un grupo de funcionarios. c) Compartir o divulgar números de cuenta, claves de acceso y número de identificación personal u otra información confidencial o sensible para la entidad.
4. Con el propósito de contar con niveles de seguridad apropiados, el funcionario deberá manejar la contraseña de acceso al correo electrónico institucional (cuando se implemente) con privacidad. En caso de que el funcionario requiera de la contraseña, ésta deberá ser solicitada por la persona a cargo de la siguiente forma: - El titular de la cuenta de correo electrónico podrá solicitar de forma escrita o verbal su clave de acceso al correo. – El funcionario a cargo será el único facultado para solicitar la clave de acceso de cualquiera de las cuentas de correo electrónico, lo cual deberá realizarse por escrito.
5. Al digitar las claves de acceso no permita que otros funcionarios adviertan cuáles son ni las comente con nadie.

DIRECCIÓN: CARRERA 7A No. 11 – 45
TELEFAX: 8616115 – 8631283 - 8616128
E-Mail:contactenos@iduvichia.gov.co
Pagina Web: www.iduvichia.gov.co

6. El buzón correo electrónico deberá ser administrado por el funcionario al cual se le ha asignado, eliminando y depurando los correos que no crea pertinentes, con el fin de no exceder su capacidad.

RESPONSABILIDADES

1. Es responsabilidad del funcionario hacer de conocimiento al personal a su cargo, sobre lo estipulado en la misma y exigir su fiel cumplimiento.
2. Funcionarios y Jefes en general deberán cumplir fielmente las disposiciones establecidas en el presente reglamento.
3. Todo funcionario es responsable de informar por escrito al funcionario a cargo sobre cualquier situación, incidente, problema de seguridad, acceso indebido o violación voluntaria o involuntaria de las normas contenidas en este reglamento.

DIRECCIÓN: CARRERA 7A No. 11 – 45
TELEFAX: 8616115 – 8631283 - 8616128
E-Mail:contactenos@iduvichia.gov.co
Pagina Web: www.iduvichia.gov.co