CONTRALORÍA
General Departamento del Chocó

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION PARA LA CONTRALORIA GENERAL DEL DEPARTAMENTO DEL CHOCO.

CONTRALORÍA
General Departamento del Chocó

INTRODUCCION

La Contraloría General del Departamento del chocó en su Plan Estratégico Institucional para el periodo 2020 - 2021 incluyó entre su slogan “la Modernización Institucional para un control Fiscal Oportuno”.

En ese orden de ideas es de total importancia hacerle conocer a sus funcionarios que en la actualidad es necesario tener los sistemas informáticos 100% seguros, esto dado a que los sistemas siempre están altamente expuestos a ataques Cibernéticos por parte de los Hackers.

Por los motivos expuestos anteriormente la Contraloría General del Departamento del Chocó optó por aprovechar al máximo sus recursos económicos y físicos, para mejorar los recursos informáticos y mantener lo más seguro posible su información. Sumado a esto la entidad aplicó las políticas de seguridad informáticas como una herramienta para concientizar a cada uno de los funcionarios en ese contexto, para que conozcan la importancia y la sensibilidad de la información reposa en sus sistemas y equipos de computación.

De igual forma Modernizar a la Entidad en cuanto a los sistemas de información y así poder ejercer un control fiscal oportuno y darle resultados a la comunidad, garantizando que los recursos sean realmente invertidos.

ALCANCE

El Plan de Seguridad y Privacidad de la Información cubren todas las áreas de la entidad y debe ser acatado tanto por la alta dirección, directivos, funcionarios y terceros que laboren o tengan relación con la Contraloría General del Departamento del Chocó, para mantener un adecuado nivel de protección y calidad de la información.

OBJETIVOS

- Describir el entorno general de la seguridad y privacidad de la información en la Contraloria General del Departamento del Chocó.

- Describir y explicar de forma detallada el MSPI que se aplica en la Contraloria General del Departamento del Chocó.

RESPONSABILIDADES

El área de Sistemas que se encuentra inmersa en la Oficina Administrativa y Financiera, se debe:

- Llevar a los comités pertinentes, socializar y lograr la aprobación del Modelo.
  - Motivar a los directivos a que se apropien del modelo.

NORMAS

- Decreto 1078 de 2015 – Define el componente de seguridad y Privacidad de la Información como parte integral de la Estrategia GEL.
- Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
- Estrategia de Gobierno Digital.

POLÍTICAS DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OBJETIVOS:

- Proteger desde el ámbito tecnológico la información institucional, los recursos informáticos y los servicios tecnológicos necesarios para que sus funcionarios puedan cumplir con sus actividades y obligaciones.
- Responsabilizar al Jefe del área de Sistemas para que se cumplan las Políticas de Seguridad de la Información.
- Controlar la calidad del servicio brindado.

PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas que estén autorizadas para tener acceso a ella.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Protección a la Duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

POLITICAS GENERALES:

- **Actualizaciones de seguridad de Windows:** Es obligación de cada funcionario permitir la descarga y actualización los parches de seguridad al sistema operativo de su computador asignado.

- **Cuenta y contraseña de usuario:** Una vez asignadas el funcionario será responsable de los eventos y actividades que se presenten con su usuario, por tal motivo se prohíbe la divulgación de contraseña a terceros.

- **Disponibilidad de los equipos:** El funcionario debe tener totalmente disponible y utilizable el equipo cuando sea requerido por parte del personal encargado.

- **Reporte de las violaciones de seguridad:** Es de carácter obligatorio para toda la planta de personal reportar inmediatamente la violación de seguridad que sea testigo, dicho reporte lo puede realizar: Por escrito, verbal o correo electrónico al responsable del área de sistemas.

- **Acceso de terceras personas a los equipos informáticos:** Deber ser autorizado, identificado, controlado y vigilado durante el acceso.

- **Manejo de datos e información:** Es responsabilidad de cada funcionario evitar la fuga de información confidencial alojada en su equipo.

- **Conexión de dispositivos USB:** Queda totalmente prohibido el uso de dispositivos USB en los equipos de Computación sin el previo análisis del antivirus.

- **Fallos en el software utilizado:** fallos imprevistos en los sistemas operativos por reinicios inesperados o mal funcionamiento de las propias herramientas de diagnóstico.

POLITICAS TECNICAS:

- Al asignar las contraseñas estas deberán tener como mínimo 8 (Ocho) caracteres que tendrán que ser alternados en letra mayúscula, letra minúscula, número y símbolo.

- Solo el área encargada del sistema proporcionara la instalación de Software de dominio público, siempre y cuando su procedencia sea de un sitio seguro.

- Asignar un área donde se ubicaran y estarán altamente protegidos los equipos de comunicaciones, Servidor y Dvr con la infraestructura apropiada de manera que solo quien esté autorizado tenga acceso físico y directo.

- Queda prohibida la conexión de componentes Hardware diferentes a los que se encuentran en su equipo asignado.

- Los equipos de uso interno deberán instalarse en lugares adecuados, lejos de polvo y humedad, evitando así su deterioro y pérdida la información almacenada.

- Cada funcionario está en la obligación de vaciar la papelera de reciclaje periódicamente, con el fin de liberar espacio en el disco duro.

- Los funcionarios tendrán acceso a Internet y deberá ser utilizado con estricta responsabilidad y sólo con fines de apoyo al cumplimiento de sus actividades institucionales teniendo en cuanta lo siguiente: No se harán descargas de archivos por internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades de la Entidad; no podrá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades propias de la Entidad; está restringido el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

- La Contraloría General del Departamento del Chocó, se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de internet de la Entidad.

- El funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

- El préstamo de portátiles, escáners, videocámaras u otro equipo informático, tendrá que solicitarse al Ingeniero encargado del área de sistemas de la Entidad.

POLITICAS DE SOFTWARE Y ALMACENAMIENTO DE DATOS:

- Todo software que se utilice deberá ser licenciado, por tal motivo todo producto sin su respectiva licencia y/o dudosa procedencia será eliminado.

- El antivirus debe estar bien configurado y actualizado para que trabaje correctamente, El antivirus no es una solución definitiva, ayuda a minimizar el riesgo.

- El servidor debe estar configurado para que realice copias de seguridad diariamente de los equipos conectados al dominio, permitiendo la recuperación de los datos cuando sea necesario.

- Se prohíbe el uso del correo electrónico institucional para el envío de contenidos diferente al utilizado por la entidad. Ejemplo: cadenas, publicidad, propaganda comercial, política, Contenidos Eróticos. Etcétera.

- Si se descubre que un empleado ha copiado información y programas informáticos de forma ilegal para dárselos a un tercero, puede ser sancionado.

- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

- Todo funcionario está obligado a proteger en la medida de sus posibilidades, los datos de carácter personal a los que tiene acceso, evitando su modificación, destrucción o mal uso.

- La responsabilidad de la reserva y la información contenida en el aplicativo contable de la entidad es totalmente del financiero.

CONTRALORÍA
General Departamento del Chocó