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

La Contraloría General del Departamento del chocó en su Plan Estratégico Institucional para el periodo 2016 – 2019 incluyó entre sus 5 objetivos estratégicos para el desarrollo de la misión y visión, el **Fortalecimiento Institucional**.

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 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.

Calle 27 Nº 6 – 40- Teléfono (094)6711334 – Fax (094)6712474
www.contraloria-choco.gov.co –Email: contactenos@contraloria-choco.gov.co

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 pares directivos y a los colaboradores de la dirección de TI 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.

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.

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.

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.

Atentamente,

Paz Leida Murillo Mena
Contralora General del Departamento del Chocó

Proyecto – Cristian Garcia

Revisó – Rosa Diaz

Calle 27 Nº 6 – 40- **Teléfono** (094)6711334 – Fax (094)6712474
www.contraloria-choco.gov.co –Email: contactenos@contraloria-choco.gov.co