POLITICAS DE SEGURIDAD INFORMATICAS

Dirección Técnica de Sistemas

Contraloría General de Boyacá

Tabla de CONTENIDO

Contenido

Audiencia

Este documento de políticas de seguridad informática está dirigido a todos los empleados, contratistas y partes involucradas en la operación y gestión de los sistemas de información de la Contraloría General de Boyacá. Su objetivo es proporcionar una guía clara y concisa sobre las medidas y prácticas de seguridad que deben ser adoptadas para proteger la información y los recursos tecnológicos de la organización.

Introducción

En un entorno digital cada vez más complejo y amenazante, la seguridad informática se ha convertido en una prioridad crítica para las organizaciones. La Contraloría General de Boyacá reconoce la importancia de salvaguardar la confidencialidad, integridad y disponibilidad de la información que maneja. Este documento establece las políticas y directrices de seguridad informática que deben ser seguidas por todos los miembros de la organización, con el fin de prevenir y mitigar riesgos de seguridad.

Justificación

La implementación de políticas de seguridad informática en la Contraloría General de Boyacá es esencial para:

- Proteger la información confidencial y sensible contra amenazas cibernéticas y físicas.
- Garantizar la continuidad operativa al prevenir interrupciones en los sistemas y la pérdida de datos.
- Cumplir con las regulaciones y normativas legales que exigen la protección de la información y la privacidad de los ciudadanos.
- Mantener la confianza de los ciudadanos y partes interesadas en la gestión de la información por parte de la Contraloría.

Glosario

A continuación, se presentan algunos términos clave utilizados en este documento:

- Confidencialidad: Garantía de que la información solo es accesible por personas autorizadas.
- Integridad: Mantenimiento de la exactitud y confiabilidad de la información a lo largo del tiempo.
- Disponibilidad: Acceso y utilización de la información y los recursos cuando se requieran.
- Cifrado: Conversión de datos en un formato ilegible para proteger su confidencialidad.
- Autenticación: Proceso para verificar la identidad de un usuario o sistema.
- Vulnerabilidad: Debilidad en un sistema que podría ser explotada por amenazas.
- Incidente de Seguridad: Evento que pone en riesgo la seguridad de la información y los sistemas.
- Política de Uso Aceptable: Reglas que establecen cómo se pueden utilizar los recursos informáticos.

Objetivos

Objetivo General

Establecer un marco integral de políticas de seguridad informática en la Contraloría General de Boyacá, con el propósito de salvaguardar la confidencialidad, integridad y disponibilidad de la información, así como prevenir y mitigar riesgos cibernéticos, garantizando el cumplimiento normativo y promoviendo una cultura de seguridad en todos los niveles de la organización.

Objetivos Específicos

- Protección de la Información Sensible: Desarrollar políticas y procedimientos para clasificar, manejar y proteger adecuadamente la información confidencial y sensible manejada por la Contraloría.
- Implementación de Controles de Acceso: Establecer mecanismos de autenticación y autorización sólidos para asegurar que el acceso a los sistemas y datos esté limitado a usuarios autorizados y con necesidad legítima.
- Prevención de Amenazas: Identificar vulnerabilidades y amenazas potenciales en los sistemas y establecer medidas de seguridad para prevenir intrusiones y ataques cibernéticos.
- Cumplimiento Normativo: Garantizar que todas las políticas de seguridad estén en conformidad con las regulaciones y normativas aplicables a la protección de la información y la privacidad.

- Respuesta a Incidentes: Establecer un plan de respuesta a incidentes que permita detectar, comunicar y mitigar de manera eficaz los eventos de seguridad, minimizando el impacto en la organización.

- Educación y Concienciación: Proporcionar programas de capacitación y concienciación en seguridad informática para todos los empleados y contratistas, fomentando una cultura de seguridad en toda la organización.

- Auditoría y Monitoreo: Establecer procedimientos de monitoreo y auditoría para supervisar la actividad de los sistemas, identificar comportamientos anómalos y garantizar el cumplimiento de las políticas de seguridad.

- Actualización Continua: Revisar y actualizar regularmente las políticas de seguridad informática para adaptarse a las nuevas amenazas y tecnologías emergentes.

POLITICAS DE SEGURIDAD INFORMATICAS

A través de las políticas informáticas se establecen los parámetros que permiten desarrollar las actividades sobre los sistemas informáticos y de información, por parte de los funcionarios en el desarrollo de procesos en las diferentes dependencias que conforman la Contraloría General de Boyacá. Los funcionarios, practicantes y contratistas autorizados para manejar equipos o sistemas de información, son responsables de cumplir con todas las políticas de la entidad relativas a la seguridad informática, en particular:

POLÍTICAS GENERALES

- Conocer y aplicar las políticas y procedimientos establecidos, en relación con el manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la entidad sin la debida autorización del Contralor General de Boyacá.
- El uso de los sistemas y equipos informáticos de la Entidad son de uso exclusivo del funcionario autorizado, quien será el responsable del mismo, además deben ser utilizados para actividades que estén directamente relacionadas con las funciones asignadas en la Dependencia.
- Reportar a la Dirección Técnica y Operativa de Sistemas, cualquier evento que pueda comprometer la seguridad de la información de la Entidad y sus recursos informáticos (contagio de virus, intrusos, modificación o pérdida de datos), para que se tomen las medidas necesarias.

POLÍTICAS ESPECÍFICAS

Políticas informáticas de hardware

- El funcionario encargado de administrar el Área de Sistemas asignara a cada funcionario un equipo de cómputo, con sesión de usuario estándar y contraseña de ingreso.
- Los equipos de escritorio de toda la Entidad deberán de estar conectados a un regulador de corriente o UPS, como medida de prevención de variaciones de electricidad.
- El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) a su cargo, protegiéndolos para disminuir el riesgo de robo, destrucción y mal uso. En caso de utilizar portátiles, se recomienda dejarlos bajo llave.
- Cualquier pérdida, robo o falla en los computadores o en la red, debe reportarse inmediatamente al funcionario encargado del Área de Sistemas, ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios
- Debe respetarse y no modificar la configuración de hardware y software establecida por la oficina de sistemas (ejemplo: fondo del escritorio del computador y demás).
- No debe ingresar al setup (área de configuración) del computador, podría desconfigurarlo y alterar su funcionamiento.
- Para llevar un equipo fuera de la Entidad se requiere diligenciar un formato de autorización de salida firmado por el Director de Sistemas o funcionario responsable.
- Se deben tener precauciones de limpieza como no consumir alimentos ni bebidas cerca del computador, para evitar el derramamiento de líquido sobre el mismo, no tocar la pantalla con los dedos ni con otros objetos y no limpie el computador o la pantalla con agua o sustancias no aptas para este tipo de elementos.

- Los servidores de red y equipos de comunicación (switches, routers, Access points,...) deben estar ubicados en sitios apropiados, protegidos contra daños y robo. Debe restringirse el acceso a éstos, así como al centro de cableado, a personas no autorizadas.
- En caso de mantenimiento de los equipos, se debe realizar copia de seguridad a los archivos de uso frecuente. La persona responsable del equipo debe verificar el correcto funcionamiento del mismo, antes y después de que se haya realizado dicho mantenimiento.

Políticas informáticas de usuarios

Estas políticas informáticas obligatorias, hacen alusión al ingreso al software y a equipos por parte de las personas que operan los sistemas de información.

- El funcionario que tenga a su cargo el computador, deberá actualizar y vacunar su equipo semanalmente con el software adecuado (antivirus) con el fin de evitar virus o amenazas informáticas, y reportar a la Dirección Técnica y Operativa de Sistemas cualquier problema o comportamiento anómalo en el desarrollo de las actividades.
- El acceso a las claves utilizadas para programas específicos de la entidad debe limitarse estrictamente a las personas autorizadas, y en ningún caso deberán revelarse a consultores, practicantes, contratistas, personal temporal, ni personas externas a la Entidad a menos que exista autorización escrita del Contralor o del Director de la Dependencia.
- La solicitud de una nueva cuenta o el cambio de privilegios (permisos) debe ser hecha por escrito y debe ser debidamente aprobada por el Contralor General de Boyacá.
- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsables de la administración o de la seguridad de los sistemas.

- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
- Cuando un empleado es despedido o renuncia a la entidad, debe desactivarse su cuenta inmediatamente deje el cargo, en todos los sistemas de información en que haya sido creada.
- Los sistemas de comunicación de la Entidad sólo deben usarse para actividades de trabajo. El acceso a programas de mensajería, o a redes sociales, se realizará en forma restringida, para propósitos relacionados con las funciones asignadas.
- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo responsabiliza al usuario de las consecuencias por las acciones que otros funcionarios realicen con esa contraseña.
- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión, en ese momento, el usuario debe escoger otra contraseña y realizar el cambio a su contraseña personal de inmediato.
- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas informáticas, pudiendo ser causal de investigaciones disciplinarias, o eventuales procesos penales por la incursión en delitos informáticos, si hay mérito para ello.

Políticas informáticas de datos e información

- No pueden extraerse datos fuera de la sede de la Entidad sin la aprobación previa del Contralor, cualquier dato que sea entregado a terceros debe contar con la respectiva autorización, de igual forma los usuarios no deben manipular la información institucional en provecho propio o de terceros. Acciones de esta naturaleza se consideran violatorias de las políticas informáticas, pudiendo ser causal de investigaciones disciplinarias o penales por la incursión en delitos informáticos, si hay mérito para ello.
- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
- Debe hacerse el respaldo de los datos guardados en computadores y servidores con la periodicidad que establezca la Dirección Técnica y Operativa de Sistemas; las copias de respaldo deben guardarse en un lugar seguro que determine la entidad, donde se encuentren a prueba de hurto, incendio, inundaciones y otros factores. Es responsabilidad del encargado de cada equipo realizar la copia de seguridad de la información de su computador personal, y el funcionario encargado del ares de sistemas se encargara de la información de los servidores y bases de datos.
- Los archivos magnéticos de información, de carácter histórico, quedarán documentados como activos de la entidad y estarán debidamente resguardados en su lugar de almacenamiento. Es obligación del responsable del equipo de cómputo, la entrega oportuna y conveniente de los archivos magnéticos de información, a quien le suceda en el cargo.

Políticas informáticas de software

- Debe instalarse y activarse una herramienta antivirus permanentemente actualizada. Si se detecta la presencia de un virus u otro agente clasificado como potencialmente peligroso, se debe notificar inmediatamente al área de Sistemas.
- No debe utilizarse ningún software bajado de Internet y en general software que provenga de una fuente no confiable, para prevenir demandas legales por derechos de autor o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado.
- Por ningún motivo se deben utilizar unidades extraíbles, sin un previo análisis de la unidad con el antivirus; esto con el fin de evitar ataques informáticos o la instalación de software malicioso que altere el comportamiento de la red y otros recursos informáticos.