



CONTRALORÍA
DEPARTAMENTAL DE BOLÍVAR

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

GENERALIDADES

La Contraloría Departamental de Bolívar, como Entidad que vigila la gestión fiscal en el Departamento de Bolívar en el ejercicio de sus deberes constitucionales se encuentra comprometida con la seguridad de la información como parte fundamental de la protección y confianza con el Estado y los ciudadanos, todo enmarcado en el cumplimiento de las leyes y en concordancia con una gestión confiable y efectiva en la vigilancia y control del uso adecuado de los recursos públicos.

En Contraloría Departamental de Bolívar, la información es un activo fundamental para el cumplimiento de las funciones misionales y de apoyo, así como para la toma de decisiones, razón por la cual, existe un compromiso expreso en su protección, como parte de una estrategia orientada a la administración de riesgos y consolidación de una cultura de seguridad, con el aseguramiento de la información se busca identificar y minimizar los riesgos a los que se expone y disminuir el impacto generado sobre sus activos, con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad, disponibilidad y privacidad de la información, acorde con las necesidades del estado, la ciudadanía, los funcionarios, terceros, proveedores, sujetos de control y en cumplimiento de las normas legales vigentes, así como, la identificación de las reglas y procedimientos que cada usuario que accede o usa los recursos tecnológicos de la Entidad debe conocer para preservar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información que usan. Estas políticas serán revisadas con regularidad, como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la Entidad, en su estructura, sus objetivos o en alguna condición que la afecte, para asegurar que dichas políticas sigan siendo adecuadas y ajustadas a los requerimientos de la Entidad.



CONTRALORÍA
DEPARTAMENTAL DE BOLÍVAR

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO GENERAL DEL SGSI

Establecer las directrices para la proteger la información de la Contraloría Departamental de Bolívar., asegurando que en ella se cumplan las características de integridad, disponibilidad y confidencialidad, mediante la ejecución de acciones en concordancia con disposiciones legales, operativas, tecnológicas y de acuerdo al objetivo estratégico, manteniendo la confianza de los usuarios internos y externos de los procesos, trámites y servicios que presta la Entidad.



TERMINOS Y DEFINICIONES

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización.

Activo de Información: en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Acuerdo de Confidencialidad: Documento donde se plasma el compromiso para mantener la confidencialidad de la información de la Entidad, a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud del desarrollo de las funciones desempeñadas en la Entidad.

Autenticación: Asegurar que una característica declarada de una Entidad es correcta.

Autenticidad: Propiedad de que una Entidad es lo que dice ser.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, Entidades o procesos no autorizados.

Dirección IP: Número que identifica, de manera lógica y jerárquica en una red informática a un dispositivo (computadora, tableta, portátil, Smartphone).

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una Entidad autorizada.

Incidente de seguridad: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información.

Información: Es un activo esencial para el negocio de una organización y por consiguiente necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato físico (por ejemplo, en papel), así como la información intangible que forma parte del conocimiento de los empleados. La información puede ser transmitida por diferentes medios incluyendo: mensajería, comunicación electrónica o verbal. Independientemente del formato o del medio por el cual se transmite la información, es necesaria siempre una protección adecuada.

Integridad: Propiedad de exactitud y completitud de la información.



CONTRALORÍA
DEPARTAMENTAL DE BOLÍVAR

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Medios removibles: Dispositivos tecnológico de almacenamiento de información diseñados para ser extraídos del computador.

Seguridad de la información: Asegura la confidencialidad, integridad y disponibilidad de la información. La seguridad de la Información implica la aplicación y gestión de controles apropiados que involucran la consideración de un amplio rango de amenazas, con el objetivo de asegurar el éxito empresarial sostenido, así como su continuidad, y minimizar las consecuencias de los incidentes de la seguridad de la información.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotada por una a más amenazas.



POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACION

La Contraloría Departamental de Bolívar. Es consciente de lo relevante de la protección de los activos de Información que soportan los diferentes procesos de la Entidad, por ello se encuentra comprometida con la implementación de medidas para asegurar su confidencialidad, integridad, disponibilidad y privacidad de acuerdo con las Lineamientos legales vigentes, para lo cual, adopta políticas, procedimientos, lineamientos y asigna responsabilidades para la adecuada gestión de la seguridad de la información”.

Así las cosas la entidad, se ha comprometido el cumplimiento de los lineamientos definidos para garantizar una adecuada seguridad de la información en el marco de confianza en el ejercicio de sus deberes con las partes interesadas, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad. Para la Contraloría Departamental de Bolívar, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

A continuación, se describen en detalle las políticas específicas de la seguridad de la información En la Contraloría Departamental de Bolívar.

DISPOSITIVOS MÓVILES

La Contraloría Departamental de Bolívar, el uso de dispositivos móviles, limitando el alcance de estos dispositivos inicialmente a los computadores portátiles (notebooks y laptops) y unidades de almacenamiento externo que contengan información de la Entidad y que a su vez se utilicen para el manejo de esta información, deben ser controlados de acuerdo al análisis de riesgo correspondiente, y mitigar el impacto a que se expone la información como su pérdida, alteración y divulgación no autorizada.

De acuerdo a lo anterior, en la entidad se establecen los siguientes lineamientos.

- Se debe contar con un inventario actualizado de dispositivos móviles (computadores portátiles y unidades de almacenamiento externo suministrados por la Entidad que no sean de consumo) utilizados para almacenar, procesar y/o transmitir información de la Contraloría.
- Se deben definir lineamientos para el acceso a redes inalámbricas, la instalación de software y/o correos electrónicos de la Entidad mediante el uso



de este tipo de dispositivos y establecerá las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles.

- Se adoptarán medidas de apoyo en seguridad de la información para ejercer correctamente la gestión de los riesgos en el acceso a la información, el procesamiento o almacenamiento que se presenten al utilizar los dispositivos móviles en lugares de trabajo remotos.
- Ante la pérdida del equipo institucional, ya sea por extravío o hurto, deberá informar de manera inmediata a la Dirección Administrativa y Financiera y continuar con el procedimiento administrativo por pérdida de elementos establecido por la Entidad.
- Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la entidad, con el fin de realizar actividades propias de su cargo o funciones asignadas en la Entidad, se debe evitar hacer uso de estos para cuestiones personales, así como en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.
- Los dispositivos móviles institucionales deben contar con mecanismos de autenticación para desbloquear el equipo y poder tener acceso a su información y servicios.
- Si desde el dispositivo móvil se procesa información se debe contar con un software instalado y actualizado contra códigos maliciosos, firewall personal para prevenir incidentes de seguridad.
- Es responsabilidad del usuario realizar periódicamente copias de respaldo a la información que se almacena en el dispositivo.

CONTROL DE ACCESO LÓGICO Y FÍSICO

En la Contraloría Departamental de Bolívar, se establecerán medidas de control de acceso a la información y demás servicios de TI, estos controles deben limitar el acceso a la información de acuerdo a la clasificación de la información, las funciones y cargos que desempeñen los funcionarios, contratistas y terceros. Siempre se brindarán accesos de acuerdo al principio de privilegio más bajo, con los cuales todos los funcionarios, contratistas y terceros puedan desempeñar correctamente sus funciones sin brindar accesos de mayor alcance a los que se requiere.

De acuerdo a lo anterior, en la entidad se establecen los siguientes lineamientos.

- Se gestionaría la elaboración de un procedimiento mediante el cual se brinden las pautas para una correcta gestión del control de acceso a usuarios en todos sus niveles; en este procedimiento se debe contemplar la restricción



y control de los accesos privilegiados a la información y los sistemas de información, así como establecer las definiciones para el monitoreo periódico de las acciones y los cambios a las cuentas privilegiadas.

- Cuando se solicite tener acceso a algún recurso o servicio de la Entidad, se deberá realizar el correspondiente análisis de riesgo con la participación del propietario de la información y de los activos asociados, con el fin de determinar los privilegios a otorgar y definir los mecanismos necesarios para su protección.
- En ningún caso se otorgará acceso a terceros, a la información, a las instalaciones, o a centros de procesamiento de información crítica, si previamente no se han cumplido los controles de seguridad establecidos.
- Se realizara una identificación de usuario (ID) para permitir que los funcionarios queden vinculados y sean responsables de sus acciones.
- Se retirara o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado de ser parte de la Entidad.
- Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debe suministrar de manera segura una contraseña temporal, la cual se debe forzar a cambiar inmediatamente realice el siguiente ingreso al sistema.
- Las contraseñas nunca se deben almacenar en sistemas de computador o en otro medio en un formato no protegido.
- El proceso de informática de la entidad establecerá los criterios para la definición de las contraseñas.
- Se debe garantizar la seguridad física de los centros de cableado incluyendo, entre otros, el sistema eléctrico y el control de acceso biométrico.
- Todas las puertas que utilicen sistema de control de acceso, deben permanecer cerradas, y es responsabilidad de todos los funcionarios y terceros autorizados evitar que las puertas se dejen abiertas.
- Todas las áreas que se hayan definido como protegidas y activos de información que la componen, deben ser protegidas de acceso no autorizado mediante controles y tecnologías de autenticación fuerte.
- En las áreas seguras donde se encuentren activos de información, se debe cumplir como mínimo con los siguientes lineamientos:
 - ❖ No se deben consumir alimentos ni bebidas.
 - ❖ No se deben ingresar elementos inflamables.
 - ❖ No se debe permitir el acceso de personal ajeno sin que este acompañado por un empleado durante el tiempo que dure su visita.
 - ❖ No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.



- ❖ No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
- ❖ No se permite el ingreso de equipos electrónicos (computadores portátiles, cámaras, celulares, USB, etc.), así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

ESCRITORIO LIMPIO Y PANTALLA LIMPIA

La Contraloría Departamental de Bolívar, establece las reglas para reducir los riesgos de acceso no autorizado, daño o pérdida, o divulgación no autorizada de la información, en cada uno de los puestos de trabajo, equipos y servidores de computo en términos de garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

De acuerdo a lo anterior, en la entidad se establecen los siguientes lineamientos.

- Los medios de copias se deben almacenar en custodia externa en una sede alterna de la Contraloría, asegurando que tenga implementado mecanismos de protección ambiental.
- Realizar pruebas de restauración de la información, de acuerdo a un plan de restauración de copias de respaldo establecido, para asegurar que se puede depender de ellos para uso de emergencia en caso necesario.
- Para la información considerada relevante o importante por cada dependencia de la Entidad, se cuenta con una unidad de almacenamiento centralizada, en la cual se almacena dicha información por los funcionarios autorizados; unidad que se encuentra incluida dentro de los esquemas de copias de respaldo implementados por la Dirección de Tecnologías de la Información de la Contraloría Departamental de Bolívar.
- Definir los tiempos de retención y de protección en instalaciones adecuadas que provean la debida seguridad física y ambiental, permitiendo minimizar el impacto de la operación de la Entidad, en caso de presentarse una falla o desastre y poder contar con la información necesaria en el momento oportuno para responder con los tiempos de restauración de los servicios.
- Se debe contar con registros exactos y completos de las copias de respaldo.
- Definir la frecuencia y tipo de copias de respaldo a realizar.
- Las pruebas de restauración se deberían hacer en medios de prueba dedicados, no sobrescribiendo el medio original, para evitar que se cause un daño o pérdida de la información



TRANSFERENCIA DE LA INFORMACIÓN

Para la transferencia de información entre la Contraloría Departamental de Bolívar y otra Entidad de cualquier orden y naturaleza sea pública, privada o mixta, se deberán establecer requisitos de confidencialidad y no divulgación de la información, para lo cual será necesario establecer los respectivos acuerdos de confidencialidad, enmarcados en las leyes vigentes. La Entidad debe implementar mecanismos y controles que permitan establecer una comunicación segura en la transferencia de la información evitando la interceptación que pueda copiar, modificar, o eliminar la información por parte de terceros.

De acuerdo a lo anterior, en la entidad se establecen los siguientes lineamientos.

- Únicamente se entrega información a receptores autorizados quienes garanticen por escrito la reserva legal y protección de la información que se les vaya a suministrar.
- Cuando proceda, la oficina responsable de dar respuesta legal a un requerimiento de información clasificada, deberá verificar previamente entre otros temas y sin limitarse a:
 - ❖ La solicitud se ajuste a la normatividad aplicable vigente.
 - ❖ La respuesta identifique el nivel de clasificación, correspondiente a la naturaleza del documento o la información que se ponga en conocimiento de la autoridad competente.
 - ❖ La respuesta cumpla con los protocolos de seguridad, acceso y reserva.
 - ❖ La respuesta con la información suministrada no debe poner en peligro o riesgo la Seguridad de la Entidad o sus funcionarios.
 - ❖ La respuesta no debe dar a conocer capacidades, procedimientos, medios, elementos técnicos, operaciones o actividades que comprometan la seguridad de la Entidad

GESTIÓN DE ACTIVOS

La Contraloría Departamental de Bolívar, debe identificar todos los activos de información, y mantener un inventario actualizado, exacto, consistente y documentado con todos los aspectos relevantes de cada uno, clasificándolos de acuerdo a la Confidencialidad, Integridad y Disponibilidad de la información, para identificar su valor y criticidad, además, cada activo debe tener un propietario que garantice los niveles de seguridad que correspondan según sea el caso.

De acuerdo a lo anterior, en la entidad se establecen los siguientes lineamientos.



- La Contraloría Departamental de Bolívar. es la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.
- Los funcionarios de la Entidad se deben comprometer a identificar, clasificar, etiquetar, disponer, devolver, y gestionar los activos de información establecidos como tal, de acuerdo a la presente política.
- Se debe mantener un registro actualizado y exacto de todos los activos de información necesarios para la prestación de servicios, de acuerdo a lo establecido en el procedimiento para la gestión de activos.
- Todos los activos de información deben tener asignado un custodio que tiene la responsabilidad de mantener los controles adecuados para su protección.
- El acceso a carpetas compartidas debe delimitarse a los funcionarios que las necesitan y deben ser protegidas con contraseñas y/o acceso por roles y responsabilidades.
- Los funcionarios y contratistas deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la Contraloría Departamental de Bolívar.
- La Contraloría de Bogotá D.C. empleará procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos.
- Los medios y equipos donde se almacena, procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

PRIVACIDAD Y CONFIDENCIALIDAD

La política de Privacidad y Confidencialidad determina los lineamientos de tratamiento y protección sobre los datos personales y sobre la información considerada como sensible y sobre la cual se deberán implementar controles de acuerdo a su nivel de clasificación.

De acuerdo a lo anterior, en la entidad se establecen los siguientes lineamientos.

- En la Contraloría Departamental de Bolívar. se deberán implementar acuerdos de confidencialidad los cuales todo funcionario, debe firmar con el



compromiso de no divulgar la información clasificada, reservada o confidencial de la Entidad.

- El ciudadano y/o funcionario reconoce que el ingreso de información personal por cualquiera de los mecanismos establecidos por la Entidad, lo realiza de manera voluntaria y ante la solicitud de requisitos específicos por la Contraloría Departamental de Bolívar. para llevar a cabo un trámite, una queja o reclamo o una solicitud o para acceder a los mecanismos interactivos que ofrece la Entidad.
- Para la recolección y tratamiento automatizado de los datos personales, como consecuencia de la navegación y/o registro por el sitio web se deberá informar al titular de los datos la finalidad de los mismos.
- Todo funcionario o tercero debe firmar un acuerdo de confidencialidad, el cual debe contener un compromiso del funcionario o tercero vinculado a la Contraloría de no divulgar la información interna y externa que conozca como parte del desarrollo de las funciones que desempeña o de su vinculación con la Entidad.
- Este acuerdo de confidencialidad debe indicar la vigencia del mismo, el cual debe mantenerse por un tiempo adicional que considere Contraloría, luego de terminada la vinculación con la Entidad.
- El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

INTEGRIDAD

La política de Integridad se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administrada por usuarios internos y externos relacionados con la Contraloría de Departamental de Bolívar.

De acuerdo a lo anterior, en la entidad se establecen los siguientes lineamientos

- Toda la información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas autorizadas y a través de los medios correspondientes, sin modificaciones ni alteraciones.
- Para la información que se clasifique como Reservada, Clasificada, Pública, y requiera ser transmitida a través de canales de comunicación se deben



utilizar mecanismos que permitan garantizar que la información mantiene su integridad mientras es transmitida por la red, es decir, que la información es completa y exacta de punto a punto en la transmisión.

CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La política de Capacitación y Sensibilización en Seguridad de la Información, se centra en formar y dar a conocer a los empleados temas relacionados con la seguridad de la información, cuya finalidad es que puedan identificar y reportar de manera oportuna los incidentes de seguridad de la información y disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

De acuerdo a lo anterior, en la entidad se establecen los siguientes lineamientos

- Se debe proveer al personal activo las habilidades requeridas a través de entrenamientos para proteger los sistemas y cumplir con las responsabilidades de administración y uso de manera oportuna, correcta y segura los activos de información.
- Se debe crear una cultura que promueva la seguridad donde todos los individuos apliquen los controles de seguridad y prevengan que la información sensible de la Entidad se vea comprometida.
- Se debe definir y desarrollar un programa de capacitación y sensibilización de tal forma que de manera periódica se refuercen los conceptos y amenazas de seguridad para que los funcionarios cuenten con información actualizada y sepan cómo actuar ante incidentes y como reportarlos.

Elaboro: Cristian Franco Castillo	Aprobó: Benjamín Azuero Angulo
Responsable Proceso de TIC	Contralor Departamental de Bolívar(e)