1. OBJETIVO

Establecer reglas y lineamientos técnicos para el uso controlado de activos de información que minimice el riesgo de pérdida de dato, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información.

2. ALCANCE

El Manual de Normas y Políticas de Seguridad Informática del **SERVICIO GEOLÓGICO COLOMBIANO** incluye a los proveedores, clientes internos que son las dependencias que componen la estructura de la Entidad y los externos que tienen vinculación mediante contratos o acuerdos interinstitucionales.

Incluye los lineamientos para proteger la información del SGC y los recursos tecnológicos con la que se procesa y se almacena, así como la recuperación de la información mantenida a nivel de medios (cintas, discos, discos ópticos, entre otros) para responder a los requerimientos de los procesos de la institución.

3. OBLIGACIONES

Es un compromiso de todos los clientes del **SERVICIO GEOLÓGICO COLOMBIANO** conocer el Manual de Normas y Políticas de Seguridad Informática y es su deber cumplirlas y respetarlas para el desarrollo de cualquier actividad TIC o consulta de sus productos.

4. PROPOSITO

El propósito que tiene el **SERVICIO GEOLÓGICO COLOMBIANO** al establecer el Manual de Normas y Políticas de Seguridad Informática es definir las normas y lineamientos a través de este documento para que la gestión de proyectos y recursos TIC se realice obedeciendo la directriz de seguridad y evitar que se creen vulnerabilidades que impacten el negocio de la Entidad.

5. BASE LEGAL

- **Ley Estatutaria 15 81 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 de 2013:** Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Decreto 2693 de 2012:** Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

- **Decreto 2578 de 2012:** Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye ñEl deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátilesò entre otras disposiciones.

- **Decreto 2609 de 2012:** Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

- **Ley 1437 de 2011:** Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- **Ley 1273 DE 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado ñde la protección de la información y los datosò y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Ley 1341 DE 2009:** Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- **Ley 1150 DE 2007:** Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.

- **BS 7799-3:2006:** Proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).

- **NTC 27001:2006:** Sistema de Gestión de Seguridad de la Información (SGSI). En 2005, con más de 1700 empresas certificadas en BS7799-2, ISO publicó este esquema como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799 y esta última norma se denomina ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de revisión.

- **ISO 27002:2005:** Esta norma proporciona recomendaciones de las mejores prácticas en la Gestión de la Seguridad de la Información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma.

- **ISO/IEC 27001:2005:** Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

- **Ley 962 DE 2005:** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

- **Modelo Estándar de Control Interno MECI 1000:2005:** Proporciona una estructura para el control de la estrategia, la gestión y la evaluación en las entidades, con el orientarlas hacia el cumplimiento de los objetivos institucionales y la contribución de estos a los fines esenciales del Estado Colombiano.

- **NTCGP1000:2004:** Esta Norma establece los requisitos para la implementación de un sistema de gestión de la calidad aplicable a la rama ejecutiva del poder público y otras entidades prestadoras de servicio.

- **ISO/IEC TR 18044:2004:** Ofrece asesoramiento y orientación sobre la Seguridad de la Información de Gestión de incidencias para los administradores de seguridad de la información y de los administradores de sistemas de información.

- **Ley 599 DE 2000:** Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

6. ADVERTENCIA

Cualquier cliente de los recursos de TIC del **SERVICIO GEOLÓGICO COLOMBIANO** que se encuentre realizando actividades que vayan en contra del Manual de Normas y Políticas de Seguridad Informática, da lugar a que la Entidad realice las investigaciones disciplinarias pertinentes y reportar a los entes de control del estado cuando haya lugar.

7. DEFINICIONES

ACTIVO: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

APLICACIONES CRITICAS: Son las aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.

BRECHA: Término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten el negocio de la Entidad.

BUENAS PRACTICAS: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.

CICLO DE VIDA DE LA INFORMACIÓN DIGITAL: Se refiere a la clasificación y almacenamiento de la información; siendo necesario tener en cuenta los requisitos técnicos y legales; así como tener claro los conceptos de disponibilidad y velocidad que depende de la misma clasificación que varía conforme su valor con el tiempo.

CLASIFICACION DE LAS APLICACIONES: Las aplicaciones se clasifican conforme los procesos de la entidad y son: Misional, Estratégico y de Apoyo.

CLASIFICACION DE LA INFORMACIÓN: Proceso formal que se utiliza para ubicar el nivel a la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

CLIENTES: Persona natural o usuario que recibe un producto Institucional. El cliente puede ser interno o externo a la organización.

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quienes esté autorizados.

CORRIENTE ELECTRICA REGULADA: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos TIC de la Entidad.

DATO: Es una letra, número o símbolo que tiende a convertirse en información.

DEPENDENCIAS: Son los grupos que conforman la estructura organizacional de la Entidad.

DISPONIBILIDAD: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

DOCUMENTO: Es el medio físico que contiene la información que se quiere transmitir.

DUEÑO DE LA INFORMACIÓN: Es cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.

INCIDENTE: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o reducción de la calidad del servicio.

INFORMACIÓN: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y que es guardada en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

INFORMACIÓN DIGITAL: Cuando la información está almacenado en un medio magnético porque cuando se imprime se convierte en documento físico y en este último caso existe en el SGC la dependencia que define los lineamientos, normas, guías y estándares.

INFORMACIÓN SENSIBLE: Es la tipificación que recibe la información que no se considerada de acceso publico como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

POLÍTICA TIC: Documento que contiene los lineamientos que define la organización para reglamentar el desarrollo de los proyectos y recursos TIC de la Entidad; como las acciones que deben permanecer en el tiempo para alcanzar los objetivos de su negocio.

POLITICA DE SEGURIDAD: Es el documento de normas y lineamientos de seguridad de la información que define la Entidad para evitar que surja vulnerabilidades que puede afectar el negocio de la Entidad.

PROCESOS CRITICOS: Concepto que se utiliza para definir el conjunto de actividades o eventos que se ejecutan bajo ciertas circunstancias que inciden en los productos misionales de la entidad y en la satisfacción de los clientes.

PROVEEDORES: Negocio o empresa que ofrece servicios a otras empresas o particulares. Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, alojamiento de aplicaciones web etc.

PROPIETARIO DE LA INFORMACION: Se utiliza para denominar a la persona autorizada para organizar, clasificar y valorar la información de su dependencia o área conforme al cargo de la estructura organizacional de la Entidad.

REPOSITORIO DE DOCUMENTOS: Sitio centralizado donde se almacena y mantiene información digital actualizada para consulta del personal autorizado.

REQUERIMIENTO: Necesidad de un servicio TIC que el usuario solicita a través del mecanismo definido por la organización en los procedimientos normalizados.

SERVICIO: Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware; así como de la Plataforma Tecnológica.

SERVICIOS TIC: El concepto de Servicio TIC consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el profesional de empresa para realizar su trabajo. Los elementos del Servicio TIC son:

- Los dispositivos: PC, portátiles, agendas electrónicas, impresoras, teléfonos, sistemas de videoconferencia, etc.

- La Red de Área Local corporativa (LAN). Así como las comunicaciones de voz incluyendo el teléfono y ahora llega el momento de proporcionar y gestionar los PC y la electrónica de red necesarios para las comunicaciones de datos.

- Las comunicaciones de voz y datos WAN (Red de Área Remota), que incluyen tanto las redes privadas corporativas como el acceso a redes públicas como Internet. La integración de las comunicaciones WAN y estas cada vez se requieren con las comunicaciones LAN.

- Los servicios y aplicaciones desde la red. Existe una clara tendencia hacia la ñexternalizaciónò de determinados servicios de acuerdo a la madurez y sus problemas conocidos y controlados. Un ejemplo es el correo electrónico. Muchas empresas prefieren ñexternalizarò este servicio para no tener que dedicar recursos a mantener y gestionar la infraestructura de correo durante las 24 horas los 7 días de la semana.

SGC: Sigla formada por las iniciales de las siguientes palabras Servicio Geológico Colombiano.

SGSI: Sistema de Gestión de Seguridad de la Información. Concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización, que debe tener la política, estructura organizativa, procedimientos, procesos y recursos necesarios para implantar la gestión de la seguridad de la información.

SISTEMA DE INFORMACIÓN: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

TIC: Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, en la actualidad no solo una computadora hace referencia al procesamiento de la información. Internet forma parte de ese procesamiento que, quizás, se realice de manera distribuida y remota.

El procesamiento remoto, además de incorporar el concepto de telecomunicación, hoy día hace referencia a un dispositivo como un teléfono móvil o una computadora ultra-portátil, con capacidad de operar en red mediante Comunicación inalámbrica.

USUARIO: Persona que utiliza los recursos TIC y que interactúan de forma activa en un proceso, secuencia, código etc.

8. CONDICIONES GENERALES

Los Directores Técnicos y Coordinadores de Grupos de Trabajo son los responsables de identificar y valorar su información; puesto que, son los propietarios de la información y el SGC es el responsable de protegerla. Todos los servidores públicos deben seguir los lineamientos enmarcados en este documento.

La seguridad de la información debe estar enmarcada con los siguientes principios:

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.

AUDITABILIDAD: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

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.

NO REPUDIO: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

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.

9. POLÍTICAS

I. POLITICA DE SEGURIDAD

1. El **SERVICIO GEOLÓGICO COLOMBIANO** debe definir los mecanismos para proteger la información, su uso, procesamiento, almacenamiento, difusión; y, es su deber, mantener actualizada la presente política así como los demás componentes del Sistema de Gestión de la Seguridad de la Información que deben estar alineados con los demás sistemas de gestión de la Entidad.
2. La Dirección de Gestión de Información Geocientífica debe dar los lineamientos para clasificar, valorar y tratamiento de la información; así como, los recursos tecnológicos involucrados.
3. La Entidad debe evaluar el costo/beneficio de los mecanismos de seguridad y recuperación de la información así como los recursos tecnológicos involucrados.

4. Todos los usuarios de los recursos TIC deben proteger, respaldar y evitar accesos de la información a personas no autorizadas; es decir son responsables de cuidar todos los activos digitales de información sean o no propiedad del SGC.
5. Todos los funcionarios del SGC deben seguir los procedimientos de respaldo de la información personal y llevar una bitácora de respaldos.
6. Todos los sistemas de información y recursos tecnológicos utilizados para el procesamiento deben contar con mecanismo de seguridad apropiados.
7. Todo usuario de TIC es responsable de la protección de la información a su cargo y no debe compartir, publicar o dejar a la vista, datos sensitivos como Usuario y Password, Direcciones IP entre otros.
8. Todo usuario de TIC debe bloquear la sesión de trabajo de su computador al alejarse aunque sea por poco tiempo, minimizando el tiempo que la estación quede sin protección en su ausencia.
9. Toda información que provenga de un archivo externo de la Entidad o que deba ser restaurado tiene que ser analizado con el antivirus institucional vigente.
10. Ningún usuario de los recursos TIC debe generar, compilar, copiar, almacenar, replicar o ejecutar código de computador malicioso con la intención de causar daño, afectar e interferir con los servicios de cualquier recurso TIC.
11. Todo usuario de los recursos TIC no debe visitar sitios restringidos por el SGC de manera explícita o implícita, o sitios que afecten la productividad en la Institución; como el acceso desde la Entidad a sitios relacionados con la pornografía, juegos etc.
12. Está prohibido descargar software de uso malicioso o documentos que brinden información que atente contra la seguridad de la información del SGC.
13. Ningún funcionario debe brindar información no autorizada en ningún sitio ya sea interno o externo de la Entidad.
14. Ningún usuario, debe descargar y/o utilizar información, archivos, imagen, sonido u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos.
15. Se documentaran y divulgaran los controles que se deben aplicar para el uso adecuado de la información que se maneja en las oficinas desde el punto de vista laboral.
16. Los usuarios no deben descargar software de Internet bajo ninguna circunstancia y en caso de requerirlo debe informar al grupo de soporte de la Entidad.

II. ORGANIZACIÓN DE LA INFORMACION

1. El **SERVICIO GEOLÓGICO COLOMBIANO** debe tener el control de su información previa organización y administración conforme la definición de su marco gerencial (funciones y responsabilidades).
2. La Dirección de Gestión de Información Geocientífica debe elaborar los documentos que contenga los lineamientos, guías y procedimientos para organizar, clasificar y valorar la información de la Entidad.
3. Cada dependencia debe determinar cuál es su información sensible y su disponibilidad.
4. Todos los usuarios de los recursos TIC de la institución deben ubicar la información que necesita ser respaldada en los lugares previamente constituidos para ello; en caso contrario son responsables de sus actos y consecuencias.
5. La Oficina Jurídica debe verificar que en todos los contratos exista el compromiso de confidencialidad de la información; así como apoyar a la Entidad para que todos los terceros cumplan con la política descrita en este documento; y, prestar la asesoría legal de la seguridad de la información necesaria.

III. CLASIFICACION DE LA INFORMACION

1. La Dirección de Gestión de Información Geocientífica debe documentar el procedimiento de Clasificación de la información como activo de la Entidad, el cual debe prevalecer los principios de

la información en las cuales se basa la seguridad como son confidencialidad, integridad y disponibilidad.

2. Todas las dependencias del **SERVICIO GEOLÓGICO COLOMBIANO** deben clasificar la información y determinar su sensibilidad y criticidad.
3. Los propietarios de la información son los encargados de clasificar la información de acuerdo con su grado de sensibilidad y criticidad; así como de documentar y mantener actualizada la clasificación, los permisos de acceso a los sistemas de información.
4. Todos los propietarios de la información deben supervisar que en su dependencia se aplique el procedimiento previamente definido en la entidad para la clasificación de la información de su competencia.
5. La Dirección de Gestión de Información Geocientífica debe apoyar al responsable de elaborar el inventario de sus activos importantes y/o asociados a cada uno de los sistemas de información; y, luego consolidar en un solo inventario dicha información.
6. El Grupo de Tecnologías de Información y Comunicaciones debe anualmente revisar el inventario de sus activos importantes y/o asociados a cada uno de los sistemas de información o cuando exista un cambio que afecte el inventario unificado.
7. La Dirección de Gestión de Información Geocientífica y el Grupo de Tecnologías de Información y Comunicaciones debe definir el procedimiento para rotular los medios tecnológicos tanto en formatos físicos como electrónicos e incluir las actividades de procesamiento como copia, almacenamiento, transmisión por correo, fax, correo electrónico. Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, entre otros) de acuerdo al esquema de clasificación que sea aprobado.

IV. SEGURIDAD DE RECURSOS HUMANOS

1. El Grupo de Tecnologías de Información y Comunicaciones debe documentar los lineamientos de seguridad que contribuya a reducir los posibles riesgos que el ser humano pueda cometer involuntariamente o voluntariamente; que incluye el uso adecuado de instalaciones y recursos tecnológicos para la seguridad de la información.
2. El **SERVICIO GEOLÓGICO COLOMBIANO** a través de su respectiva dependencia de Talento Humano y la Oficina de Contratos y Convenios debe informar al personal nuevo que se vincule o contrate en la Entidad la existencia del Manual de Políticas de Seguridad de la Información e incluir en los contratos de estos últimos, el compromiso de confidencialidad de la información y la responsabilidad en materia de seguridad.
3. El **SERVICIO GEOLÓGICO COLOMBIANO** a través de la dependencia de Talento Humano debe capacitar permanentemente a los usuarios o clientes internos en materia de seguridad de la información y difundir las posibles amenazas y riesgos que afectan los recursos TIC de la Entidad.
4. El Grupo de Tecnologías de Información y Comunicaciones debe realizar permanentemente campañas de seguridad de la información, dirigidas a todos los usuarios o clientes de los recursos TIC y fomentar el cambio culturar para evitar que las personas realicen descargas de archivos de Internet como de software espía, los troyanos y los atacantes externos etc., y que accedan a sitios desconocidos o de baja confianza, entre otros.

V. SEGURIDAD FISICA AMBIENTAL

1. El **SERVICIO GEOLÓGICO COLOMBIANO** a través del Grupo de Servicios Administrativos debe garantizar la seguridad física en todas las sedes de la Entidad para prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones así como a la información que recibe y genera el Instituto.
2. Todos los recursos físicos inherentes a los sistemas de información del SGC como las instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc. deben estar protegidos.

3. Los recursos TIC utilizados para el procesamiento de la información deben ser ubicados en sitios estratégicos con mecanismos de seguridad que permita controlar el acceso solo a las personas autorizadas e incluir en la protección de los mismos los traslados por motivos de mantenimiento u otros escenarios.
4. El SGC a través de las diferentes dependencias debe identificar y garantizar el control de los aspectos ambientales que pueden llegar a interferir el correcto funcionamiento de los recursos tecnológicos inherentes en el procesamiento y almacenamiento de la información institucional.
5. Todas las Dependencias del SGC deben definir los niveles de seguridad física en las instalaciones de sus oficinas que está bajo su responsabilidad y como Propietarios de la Información son los encargados de aprobar o negar la autorización formal del acceso a las oficinas de su competencia cuando sea requerido.
6. Todos los usuarios y clientes internos de la Entidad son responsables del uso adecuado de las pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario que realiza.

VI. GESTION DE COMUNICACIONES/OPERACIONES

1. El Grupo de Tecnologías de Información y Comunicaciones debe garantizar el correcto funcionamiento y seguro de todas las operaciones que se realizan en el Data Center de la Entidad con relación al procesamiento de la información y comunicaciones.
2. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de definir las responsabilidades funcionales y operativas con relación al Data Center y de que se documente los procedimientos para su gestión y operación.
3. El Grupo de Tecnologías de Información y Comunicaciones y el Profesional de Seguridad Informática y los Propietarios de la Información de cada una de las Dependencias deben definir y documentar los requerimientos para resguardar la información por la cual es responsable.
4. El Grupo de Tecnologías de Información y Comunicaciones debe aprobar y documentar el procedimiento relacionado con los servicios para transportar la información cuando sea demandado, de acuerdo a su nivel de criticidad.
5. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de mantener actualizados los procedimientos operativos identificados en esta Política.
6. El Grupo de Tecnologías de Información y Comunicaciones debe definir los procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.
7. El Profesional de Seguridad Informática debe verificar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan.
8. El Grupo de Tecnologías de Información y Comunicaciones debe analizar con su equipo el posible impacto operativo de los cambios previstos y verificar su correcta implementación.
9. Los responsables de la gestión operativa y de comunicaciones del Data Center deben evaluar los riesgos y determinar los controles que se deben implementar, realizar monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.
10. Las actividades relacionadas con el ambiente de Desarrollo, Prueba y Operaciones se deben realizar siempre que sea posible en instalaciones físicas diferentes y definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.
11. La administración de las instalaciones de procesamiento o las operaciones que se encuentren tercerizados en instalaciones externas a la de la Entidad deben incluir los controles y estar soportadas en el contrato de tercerización.
12. El Grupo de Tecnologías de Información y Comunicaciones debe efectuar el monitoreo al crecimiento del volumen de la información de los sistemas que se encuentran en operación en el Data Center y evaluar la capacidad de almacenamiento y procesamiento de los recursos utilizados, con el fin de proyectar el alcance de estos para evitar saturación en los mismos.

13. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de evaluar los posibles cuellos de botella, que puedan generar amenaza a la seguridad o a la continuidad del procesamiento; también debe planificar la acción correctiva que corresponda.
14. El Grupo de Tecnologías de Información y Comunicaciones y el Profesional de Seguridad Informática deben elaborar y documentar los procedimientos y definir los criterios para aprobar los nuevos sistemas de información, actualizaciones y nuevas versiones e incluir el procedimiento para la ejecución de las pruebas y aprobación final.
15. El Grupo de Tecnologías de Información y Comunicaciones con la asesoría del profesional de Seguridad Informática deben definir los controles para la protección contra el software malicioso.
16. La Dirección de Gestión de Información Geocientífica, el profesional de Seguridad Informática y los Propietarios de Información deben determinar los requerimientos para proteger cada software o dato en función de su clasificación y valor para la entidad o la criticidad de la misma.
17. El Grupo de Tecnologías de Información y Comunicaciones, el profesional de Seguridad Informática deben definir y documentar el esquema de resguardo de la información.
18. El Grupo de Tecnologías de Información y Comunicaciones debe llevar el control de los registros tales como los intentos de acceso a los sistemas, tiempo de inicio y cierre del mismo, errores y medidas correctivas tomadas, entre otras actividades que realiza el personal operativo y de comunicaciones.
19. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de documentar e implementar los controles de seguridad de los datos y los servicios conectados en las redes de la Entidad.
20. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de administrar y documentar los procedimientos de Medios Informáticos removibles, como cintas, discos, casetes entre otros.
21. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de definir y documentar los procedimientos para la eliminación segura de los medios de información acorde a la normatividad que se encuentre vigente.
22. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de definir los procedimientos para la Clasificación y el Manejo y Almacenamiento de la Información y restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.
23. Cuando exista acuerdos entre las Entidades para el intercambio de información y software, se debe documentar las especificaciones del grado de sensibilidad de la información y las consideraciones de seguridad que se deben aplicar.
24. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de documentar los procedimientos relacionados con el transporte de medios informáticos a fin de proteger la información sensible contra divulgación o modificación no autorizadas.
25. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de documentar e implementar los controles para reducir los riesgos de incidentes de seguridad en el correo electrónico.
26. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de definir y documentar las normas y procedimientos relacionados con el uso adecuado del Correo Electrónico que debe incluir protección de archivos adjuntos de correo electrónico, uso de técnicas criptográficas para proteger la confidencialidad e integridad, de los mensajes electrónicos, retención de mensajes que se deben almacenar y como deben ser usados en caso de ser requeridos legalmente.
27. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de definir e implementar los controles relacionados con el uso adecuado del Correo Electrónico.
28. La Dirección de Gestión de Información Geocientífica es la encargada de definir los aspectos operativos para garantizar el correcto funcionamiento del servicio como el tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, definición de los alcances del uso del correo electrónico por parte del personal de la Entidad entre otros.

29. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de documentar los procedimientos de operatividad de los Sistemas Electrónicos de Oficina así como de implementar los mecanismos de control para la distribución y difusión de los mismos.
30. La Dirección de Gestión de Información Geocientífica es la encargada de desarrollar e implementar procedimientos para la interacción u operatividad y comunicación de la información que tiene interconexión con el acceso público de sistemas de información del negocio de la Entidad.
31. La Dirección de Gestión de Información Geocientífica es la encargada de desarrollar e implementar procedimientos para regular y proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

VII. ACCESO A LOS RECURSOS TIC

1. El Grupo de Tecnologías de Información y Comunicaciones debe documentar y revisar los procedimientos para administrar y controlar el acceso a los sistemas y recursos tecnológicos de la Entidad de acuerdo a las necesidades de seguridad y de su negocio.
2. La dependencia propietaria de la información debe solicitar a la Dirección de Gestión de Información Geocientífica los usuarios y perfiles para el acceso autorizado a los sistemas de información de su respectiva área cuando se requiera.
3. La dependencia propietaria de la información es la encargada de mantener la integridad y confidencialidad de los datos de los sistemas de información que maneja.
4. Todo usuario de los recursos TIC debe advertir la Dirección de Gestión de Información Geocientífica que información requiere medidas específicas de protección para evitar el acceso al personal no autorizado.
5. Todos los usuarios de TIC que utilicen medios de almacenamiento de información como CDs, Dvds, Memorias USB, Portátiles, Discos externos deben utilizar en todo momento las guías que estén documentadas para su uso adecuado aunque haya terminado la sesión de trabajo.
6. Los accesos a los servicios de correo electrónico y de Intranet deben ser solicitado por el Funcionario Autorizado a la Dirección de Gestión de Información Geocientífica conforme al procedimiento formalizado.
7. El Grupo de Tecnologías de Información y Comunicaciones debe documentar de manera formal la administración de Contraseñas de Usuario de acceso a los sistemas de información y de aquellas con las cuales se realizan actividades criticas como instalación de plataformas, habilitación de servicios, actualización de software, configuración de componentes informáticos, entre otros; y, que deben encontrarse protegidas por contraseñas con un mayor grado de complejidad de seguridad.
8. El Propietario de la Información debe proteger y controlar el acceso a los datos y servicios de información conforme al procedimiento formal establecido en la Entidad.
9. Los usuarios deben seguir y aplicar las buenas prácticas de seguridad para la selección y uso de contraseñas que la Subdirección de Información Geológica implante y documente.
10. El Grupo de Tecnologías de Información y Comunicaciones debe reglamentar el acceso a los equipos como estaciones de trabajo o servidores de archivos que se encuentren instalados en las áreas de usuario para que solo el usuario autorizado tenga acceso a ellos.
11. El Grupo de Tecnologías de Información y Comunicaciones debe documentar el procedimiento para el acceso a los servicios de red tanto internos como externos e incluir los controles de seguridad que contribuya a disminuir el riesgo de acceso no autorizado.
12. El Grupo de Tecnologías de Información y Comunicaciones debe documentar e implementar las opciones para acceder y controlar la ruta entre la terminal de usuario y los servicios a los cuales se encuentra autorizado utilizar.
13. El Grupo de Tecnologías de Información y Comunicaciones en conjunto con el Propietario de la Información de cada una de las dependencias deben evaluar los riesgos para el acceso de los sistemas de información e implementar mecanismo de control como una autenticación segura.

14. El Grupo de Tecnologías de Información y Comunicaciones debe documentar y controlar la conexión remota y el acceso a los sistemas de información de la Entidad con el fin de minimizar el riesgo de accesos no autorizados.
15. El Grupo de Tecnologías de Información y Comunicaciones debe administrar, controlar y documentar los perímetros de seguridad que implemente mediante la instalación y configuración de ñgatewaysò con funcionalidades de ñfirewallò o redes privadas virtuales, para filtrar el tráfico entre los dominios y bloquear el acceso no autorizado.
16. El Funcionario Autorizado debe solicitar al Grupo de Tecnologías de Información y Comunicaciones el acceso a Internet y demás servicios conforme lo reglamentado en el procedimiento y la la Dirección de Gestión de Información Geocientífica es la responsable de implementar las reglas de seguridad como limitar el acceso a los sitios Web que vayan en contra de los derechos constitucionales y el buen nombre de la Entidad.
17. El Grupo de Tecnologías de Información y Comunicaciones debe documentar los procedimientos e implementar controles relacionados con el ruteo de redes, las conexiones informáticas y los flujos de información. Estos controles deben incluir como mínimo verificar positivamente las direcciones de origen y destino así como los dispositivos de red tales como Hubs, Switches, Bridges, Modems o Routers que tenga la Plataforma Tecnológica en la Entidad.
18. En los procedimientos que el Grupo de Tecnologías de Información y Comunicaciones documente debe definir las pautas para garantizar la seguridad de los servicios de redes tanto públicos como privados de la Entidad.
19. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de evaluar y documentar el riesgo de acceder al sistema operativo de forma insegura y determinar el procedimiento de conexión segura al sistema informático con el fin de reducir el riesgo de accesos no autorizados.
20. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de documentar y controlar el Uso de Utilitarios de Sistema que pueden tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso debe ser limitado y minuciosamente controlado.
21. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de documentar, reglamentar y controlar la Identificación y Autenticación de los Usuarios. Se debe optar por una técnica de autenticación adecuada para verificar y validar la identidad pedida por el usuario.
22. El Grupo de Tecnologías de Información y Comunicaciones junto con los Propietarios de Información deben determinar las terminales que consideren en alto riesgo o que sirven a un sistema de alto riesgo; y, detallar las reglas que se deben aplicar en un periodo definido de inactividad con el fin de minimizar el riesgo de seguridad del área y de la información que maneje la terminal.
23. Se debe fomentar la desconexión por tiempo sin uso temporal de los computadores personales activos en las oficinas o que se active el protector de pantalla con contraseñas y evite el acceso no autorizado, sin cerrar las sesiones de aplicación o de red si debe abandonar su puesto de trabajo momentáneamente. De igual forma, se debe definir limitaciones en el tiempo de conexión que proporcionen un nivel de seguridad adicional a las aplicaciones de alto riesgo.
24. Debe estar restringido el acceso a las aplicaciones o sistemas de información e inclusión del personal de soporte, quienes pueden tener acceso a la información y a las funciones de los sistemas de aplicación de conformidad con los procedimientos documentados por el Grupo de Tecnologías de Información y Comunicaciones.
25. El Grupo de Tecnologías de Información y Comunicaciones debe evaluar los sistemas y determinar lo que son sensibles y requieren de un ambiente informático dedicado o aislado o que sólo debe compartir recursos con los sistemas de aplicación confiables o no tener limitaciones.
26. El Grupo de Tecnologías de Información y Comunicaciones debe documentar los procedimientos para el manejo de dispositivos de computación móvil y trabajo remoto que incluyan la protección física necesaria, el acceso seguro y la utilización de los dispositivos en lugares públicos, el acceso a los sistemas de información y servicios a través de estos y la protección contra software malicioso.

27. El Grupo de Tecnologías de Información y Comunicaciones debe documentar los procedimientos para el uso adecuado de dispositivos móviles e incluir la protección física necesario, el acceso seguro a los dispositivos, la utilización en lugares públicos. el acceso a los sistemas de información y servicios de la Organización a través de estos equipos, así como los mecanismos de Seguridad de la Información contenida en ellos y la protección contra software malicioso.
28. El trabajo remoto sólo debe ser autorizado por el Grupo de Tecnologías de Información y Comunicaciones, una vez que el Propietario de la Información o superior jerárquico correspondiente, solicita el servicio conforme el procedimiento. La Dirección de Gestión de Información Geocientífica debe evaluar las medidas de protección que correspondan a la Seguridad de la Información, normas y procedimientos existentes.

VIII. ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

1. El Grupo de Tecnologías de Información y Comunicaciones debe documentar los procedimientos para adquirir nuevos desarrollos de software y a las mejoras o actualizaciones e incluir los mecanismos de control.
2. La Política aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes donde aplique.
3. El Grupo de Tecnologías de Información y Comunicaciones junto con el Propietario de la Información deben determinar la criticidad de la información para definir los requerimientos de protección como métodos criptográficos a ser utilizados.
4. Los Requerimientos de Seguridad de los Sistemas de Información deben ser enviados a la El Grupo de Tecnologías de Información y Comunicaciones, con el fin de que se realice el análisis y evaluación de requisitos técnicos para determinar la viabilidad de la solución.
5. El procedimiento para el desarrollo de nuevos sistemas, actualización o mantenimiento debe incluir controles en las diferentes etapas del proceso tales como en el análisis y diseño que permita evaluar el avance del sistema, así como detectar las posibles fallas potenciales de diseño y estructural que deben ser corregidos a tiempo antes de que sea implementado.
6. El Grupo de Tecnologías de Información y Comunicaciones debe documentar los procedimientos que confirme que la salida de los datos de las aplicaciones son los esperados y que el procesamiento determina la exactitud, precisión y clasificación de la información proyectada. También incluir las responsabilidades de todo el personal involucrado en este proceso.
7. Toda Aplicación que incluya el envío de mensajes o correos electrónicos debe ser evaluada que información contiene, determinar su clasificación y considerar la implementación de controles criptográficos según sea la criticidad de esta.
8. El Grupo de Tecnologías de Información y Comunicaciones debe evaluar y documentar en que situaciones hay que utilizar sistemas y técnicas criptográficas para proteger la información previo análisis de riesgo efectuado que asegure una adecuada protección de su confidencialidad e integridad.
9. El Propietario de la Información y la El Grupo de Tecnologías de Información y Comunicaciones deben realizar evaluación de riesgos e identificar el nivel requerido de protección del nuevo sistema, actualización o mantenimiento, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas que se vaya a utilizar.
10. El Grupo de Tecnologías de Información y Comunicaciones debe documentar e implementar mecanismo de seguridad para proteger la confidencialidad de las claves privadas. Asimismo, incluir la integridad de la clave pública. Esta protección se puede proveer mediante el uso de un certificado de clave pública.
11. El Grupo de Tecnologías de Información y Comunicaciones debe documentar procedimientos relacionados con Servicios de No Repudio con el fin de proporcionar herramientas que evite que se niegue haberla efectuado y resolver alguna discrepancia acerca de la ocurrencia de un evento o acción.

12. El Grupo de Tecnologías de Información y Comunicaciones debe proporcionar una protección adecuada al sistema que utiliza para generar, almacenar y archivar claves, que considere crítico o de alto riesgo y que puedan ser protegidas contra modificación, destrucción o copia o divulgación no autorizada.
13. El Grupo de Tecnologías de Información y Comunicaciones debe garantizar que los desarrollos y actividades de soporte a los sistemas adquiridos o actualizados se lleven a cabo de manera segura con los controles necesarios para permitir el acceso a los archivos solo al personal autorizado.
14. Toda aplicación o desarrollo que adquiera la Entidad de un tercero debe tener un único responsable, el cual es sugerido por el Grupo de Tecnologías de Información y Comunicaciones y designado formalmente.
15. Las empresas desarrolladoras del nuevo sistema así como los programadores o analistas de desarrollo y mantenimiento de aplicaciones deben trabajar en un esquema de pruebas y no acceder a los ambientes de producción.
16. Las pruebas de los sistemas se deben ser efectuadas en conjunto con los Propietarios de la Información y la Dirección de Gestión de Información Geocientífica sobre datos extraídos del ambiente operativo conforme las normas y procedimientos que se defina.
17. El Grupo de Tecnologías de Información y Comunicaciones debe definir el procedimiento para reglamentar el proceso para la implementación de nuevos sistemas.
18. El Grupo de Tecnologías de Información y Comunicaciones debe documentar el procedimiento de Control de Cambios de Datos Operativos con el fin de que cualquier modificación, actualización o eliminación solo se realice a través de los sistemas que los procesan.
19. El Grupo de Tecnologías de Información y Comunicaciones debe garantizar el Control de Acceso a las Bibliotecas de Programas Fuentes y asignar el responsable de su custodia.
20. En el Procedimiento de Seguridad de los Procesos de Desarrollo y Soporte que documente el Grupo de Tecnologías de Información y Comunicaciones debe incluir los controles necesarios para la implementación de cambios imponiendo el cumplimiento de los procedimientos formales que garantice la seguridad y control conforme la división de funciones incluidas.
21. Todo cambio que requiera efectuarse en el Sistema Operativo debe ser evaluado en el Grupo de Tecnologías de Información y Comunicaciones con el fin de analizar el impacto que pueda incidir en el funcionamiento o seguridad de los nuevos sistemas adquiridos o desarrollados bajo este esquema.
22. La modificación de paquetes de software suministrados por terceros deben ser comunicados a el Grupo de Tecnologías de Información y Comunicaciones previa autorización del Propietario de la Información conforme al procedimiento para controlar el Cambio de Paquetes de Software, el cual debe contemplar el análisis de los términos y condiciones de la licencia y conocer que modificaciones se encuentran autorizadas; así como determinar la conveniencia de la modificación y los responsables para evaluar el impacto que puede darse sobre cada uno de ellos y por seguridad realizar estos cambios sobre una copia.
23. Se debe reglamentar en el procedimiento para adquirir programas para que se efectúe a proveedores acreditados y que los productos sean evaluados previamente así como revisar el código fuente (cuando sea posible) antes de utilizar los programas, controlar el acceso y las modificaciones y también incluir herramientas de control infección del software con código malicioso.
24. Se debe reglamentar la adquisición de Software e incluir los controles necesarios para verificar la Propiedad de Código y derechos conferidos, licencias, acuerdos así como los requerimientos contractuales con respecto a la calidad del mismo y la existencia de garantías, la certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, así como las auditorías y revisión de código para detectar código malicioso, verificar el cumplimiento de los requerimientos de seguridad del software establecidos, así como el desempeño de las condiciones de seguridad en Contratos de Tercerización entre otros aspectos.

IX. INCIDENTES DE SEGURIDAD DE LA INFORMACION

1. Se debe establecer un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento debe incluir la detección de un supuesto incidente o violación de la seguridad e indicar los recursos necesarios para la investigación y resolución del incidente, y el responsable de realizar el monitoreo. Asimismo, debe mantener informado al Grupo de Tecnologías de Información y Comunicaciones de la ocurrencia de incidentes de seguridad.
2. Cada usuario que tiene acceso a un Equipo de Respuesta a Incidentes de Seguridad Informática debe conocer los servicios e interacciones de este equipo mucho antes de que se presente el evento que atente contra la Confidencialidad, Integridad y Disponibilidad de la información y realizar monitoreo para sugerir los controles que contribuya a minimizar el impacto de que se materialice el incidente.
3. El Grupo de Tecnologías de Información y Comunicaciones debe implementar las herramientas y mecanismos necesarios para fomentar una buena comunicación entre las dependencias o clientes para conocer las posibles debilidades en materia de seguridad, así como de los incidentes ocurridos, con el fin de minimizar sus efectos y prevenir su reincidencia.
4. Toda la información de incidentes de seguridad se debe registrar, evaluar e identificar aquellos que son recurrentes o de alto impacto; así como establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.
5. El Grupo de Tecnologías de Información y Comunicaciones debe establecer las funciones y procedimientos para el manejo de incidentes que garantice una respuesta rápida, eficaz y sistemática a los incidentes relativos a la seguridad.
6. Se debe llevar registros de auditoría el cual debe incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y a otros recursos.
7. Se debe realizar un informe de las amenazas detectadas contra los sistemas; el cual debe estar incluido en el procedimiento de registro y revisión de eventos detectados en la auditoría.
8. El Grupo de Tecnologías de Información y Comunicaciones debe establecer la periodicidad de dichas revisiones o auditorias de acuerdo a la evaluación de riesgos que efectúe en conjunto con los Propietarios de la Información.
9. El Grupo de Tecnologías de Información y Comunicaciones debe coordinar la correcta configuración para la sincronización de relojes en el equipo que vaya a realizar estos registros de auditoria para ello debe incluir dentro del procedimiento el ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

X. CONTINUIDAD DEL NEGOCIO

1. La administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo del **SERVICIO GEOLÓGICO COLOMBIANO**.
2. Los Directivos del SGC deben definir las pautas para el correcto análisis y evaluación de los riesgos de seguridad de la información así como identificar el nivel del impacto y gestionar las diferentes estrategias para el tratamiento de tal forma que garantice la continuidad e integridad de los sistemas de información del negocio de la Entidad.
3. Se debe documentar los procedimientos que contribuya a minimizar los efectos de las posibles interrupciones de las actividades normales de la Entidad (sean éstas resultado de desastres naturales, accidentales, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
4. Se debe analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para prevenir hechos similares en el futuro.
5. Se debe documentar los procedimientos que buscan maximizar la efectividad de las operaciones de contingencia en la Entidad con el establecimiento de planes que incluyan al menos las etapas de

Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan, Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original y la Recuperación: que consiste en restaurar las capacidades de proceso del sistema a las condiciones de operación normales.

6. Se debe definir las funciones para cada actividad definida y las responsabilidades tanto de la coordinación como del personal de la Entidad que participa en el proceso así como documentar los contactos externos que participarán en las estrategias de planificación de contingencias.
7. El Grupo de Tecnologías de Información y Comunicaciones debe participar de manera activa en la definición, documentación, prueba y actualización de los planes de contingencia; de igual forma los Propietarios de la Información y el profesional de Seguridad Informática.
8. Se debe identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del negocio de la Entidad, así como evaluar los riesgos para determinar el impacto de dichas interrupciones e identificar los controles preventivos.
9. Se debe desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de los sistemas y actividades del negocio de la Entidad.
10. Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del negocio de la Entidad.

XI. CUMPLIMIENTO DE NORMAS POLITICAS DE SEGURIDAD DE INFORMACION

1. La divulgación del Manual de Normas y Políticas de Seguridad Informático debe ser transmitido e implementado a través de las diferentes dependencias que conforman la estructura organizacional y jerarquía del SGC con el debido contexto.

2. Todos los clientes del **SERVICIO GEOLÓGICO COLOMBIANO** o proveedores que se encuentren en el nivel de servicios TIC deben estar autorizados por el Grupo de Tecnologías de Información y Comunicaciones para el uso de los recursos TIC quien debe vigilar el uso adecuado de la información y de toda la plataforma tecnológica.

3. La Dependencia de Talento Humano por medio del Grupo de Tecnologías de Información y Comunicaciones debe brindar capacitación a toda a la Entidad sobre los riesgos y amenazas que puede tener la información el cual se considera un activo valioso para el SGC y la conveniencia de aplicar las políticas de seguridad Informática para evitar vulnerabilidades que impacten a la entidad.

4. El Grupo de Tecnologías de Información y Comunicaciones es la encargada de socializar en todas las dependencias los lineamientos aprobados por el Comité de Seguridad de la Información sobre el proceso y procedimiento para la clasificación de la información.

5. Todas las dependencias deben adoptar y cumplir las normas y lineamientos que emita el Comité de Seguridad de la Información para la administración de las copias de seguridad.

XII. EXCEPCIONES

Toda solicitud de excepción de alguna política debe ser solicitada al Grupo de Tecnologías de Información y Comunicaciones con la debida justificación y documentación conforme la naturaleza de su cargo o dadopor eventos no contemplados en este Manual de Normas y Políticas de Seguridad Informática; previa evaluación del alcance y el impacto.

La evaluación de la excepción puede requerir el apoyo de la Oficina Jurídica, Oficina de Control Interno, Grupo de Planeación y/o Secretaría General