



Gobernación del Archipiélago
de San Andrés, Providencia y Santa Catalina

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 2.3 de 2022

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 2 de 54

Tabla de contenido

1. INTRODUCCIÓN	8
1.1 Objetivo	8
1.2 Términos y definiciones	9
1.3 Alcance y aplicabilidad.....	10
1.4 Nivel de Cumplimiento	10
1.5 Estructura del documento de políticas de seguridad	10
2 GESTIÓN Y TRATAMIENTO DE ACTIVOS DE INFORMACIÓN	11
2.1 Principal concepto de activos de información	11
2.2 Incidente de seguridad	12
3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	13
3.1 Directrices de la Dirección en seguridad de la información.	13
3.1.1 Conjunto de políticas para la seguridad de la información	13
3.1.2 Revisión de las políticas de seguridad de la información.....	14
4. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.....	14
4.1 Entidad interna.....	14
4.1.1 Asignación de responsabilidades para la seguridad de la información.	15
4.1.2 Segregación de las tareas	15
4.1.3 Contacto con las autoridades	15
4.1.4 Contacto con grupos de interés especial	15
4.1.5 Seguridad de la información en la gestión de proyectos.....	16
4.2 Dispositivos para movilidad y el teletrabajo	16
4.2.1 Política de uso de dispositivos para movilidad.....	16
4.2.2 Teletrabajo	16
5. SEGURIDAD DE LOS RECURSOS HUMANOS	17
5.1 Antes de la contratación	17
5.1.1 Investigación de antecedentes	17
5.1.2 Términos y condiciones de contratación.....	17
5.2 Durante la contratación y/o empleo.....	17
5.2.1 Responsabilidades de gestión	17
5.2.2 Concientización, educación y formación en la seguridad de la información	18

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 3 de 54

5.2.3 Proceso disciplinario.....	18
5.3 Terminación o cambio de empleo.....	18
5.3.1 Terminación o cambio de puesto de trabajo	18
6. GESTIÓN DE ACTIVOS	19
6.1 Responsabilidad sobre los activos	19
6.1.1 Inventario de activos.....	19
6.1.2 Propiedad de los activos	19
6.1.3 Uso aceptable de los activos	19
6.1.4 Devolución de los activos	19
6.2 Clasificación de la información	19
6.2.1 Directrices de clasificación	19
6.2.2 Etiquetado y manipulado de la información	22
6.2.3 Manipulación de activos	22
6.3 Manejo de los soportes de almacenamiento	22
6.3.1 Gestión de soportes extraíbles	22
6.3.2 Eliminación de soportes.	22
6.3.3 Soportes físicos en tránsito	22
7. CONTROL DE ACCESO	23
7.1 Requisitos de negocio para el Control de acceso.....	23
7.1.1 Política de Control de acceso	23
7.1.2 Control de acceso a las redes y servicios asociados	24
7.2 Gestión de acceso de usuarios	24
7.2.1 Gestión de altas y bajas en el registro de usuarios.....	24
7.2.2 Gestión de los derechos de acceso asignados a los usuarios.....	24
7.2.3 Gestión de derechos de acceso privilegios especiales	25
7.2.4 Gestión de información confidencial de autenticación de los usuarios.....	25
7.2.5 Revisión de los derechos de acceso de los usuarios.....	26
7.2.6 Retirada o adaptación de los derechos de acceso	26
7.3 Responsabilidades de los usuarios	26
7.3.1 Uso de la información confidencial para la autenticación.....	26
7.4 Control de acceso a sistemas y aplicaciones.....	26
7.4.1 Restricción del acceso a la información.....	27
7.4.2 Procedimientos seguros de inicio de sesión.	27
7.4.3 Sistema de gestión de contraseñas.....	27
7.4.4 Uso de herramientas de administración de sistemas.....	27
7.4.5 Control de acceso al código fuente de los programas	27

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 4 de 54

8. CIFRADO	28
8.1 Controles criptográficos	28
8.1.1 Política sobre el uso de controles criptográficos	28
8.1.2 Administración de claves	28
9. LA SEGURIDAD FÍSICA Y AMBIENTAL	28
9.1 Áreas seguras	28
9.1.1 Perímetro de seguridad física	28
9.1.2 Controles físicos de entradas	29
9.1.3 Seguridad de oficinas, despachos, salas e instalaciones	30
9.1.4 Protección contra las amenazas externas y ambientales	31
9.1.5 Trabajar en áreas seguras.....	31
9.1.6 Áreas de acceso público carga y descarga	32
9.2 Seguridad de los Equipos	32
9.2.1 Emplazamiento y Protección del equipo	32
9.2.2 Instalaciones de suministro	33
9.2.3 Seguridad del cableado.....	33
9.2.4 Mantenimiento de los equipos	33
9.2.5 Salida de los activos fuera de las dependencias de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	33
9.2.6 Seguridad de los equipos y de los activos fuera de las instalaciones	33
9.2.7 Reutilización o eliminación segura de dispositivos de almacenamiento.....	33
9.2.8 Equipo informático de usuario desatendido	33
9.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	34
10 SEGURIDAD EN LA OPERACIONES	34
10.1 Responsabilidades y Procedimientos de operación	34
10.1.1 Documentación de Procedimientos de operación	35
10.1.2 Gestión de cambios.....	35
10.1.3 Gestión de capacidades	36
10.1.4 Separación de entornos de desarrollo, prueba y producción	36
10.2 Protección contra código malicioso	36
10.2.1 Controles contra el código malicioso	36
10.3 Copias de Seguridad	37
10.3.1 Copias de seguridad de la información.....	37
10.4 Registro de actividad y supervisión	39
10.4.1 Registro y gestión de eventos de actividad.....	39
10.4.2 Protección de los registros de información	39

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 5 de 54

10.4.3 Registros de actividad del administrador y operador del sistema.....	39
10.4.4 Sincronización de relojes.....	39
10.5 Control de software en explotación.....	39
10.5.1 Instalación del software en sistemas en producción	39
10.6 Gestión de vulnerabilidades técnicas	39
10.6.1 Gestión de las vulnerabilidades técnicas	39
10.6.2 Restricciones en la instalación de software	39
10.7 Consideraciones de las auditorías de los sistemas de información.....	40
10.7.1 Controles de auditoría de sistemas de información	40
11. SEGURIDAD DE LAS COMUNICACIONES	40
11.1 Gestión de la seguridad en las redes	40
11.1.1 Controles de red.....	40
11.1.2 Mecanismos de Seguridad asociados a servicios en red.....	40
11.1.3 Segregación de redes	40
11.2 Intercambio de información con partes externas.....	41
11.2.1 Políticas y procedimientos de intercambio de información.....	41
11.2.2 Acuerdos sobre la transferencia de información	41
11.2.3 Mensajería electrónica	42
11.2.4 Acuerdos de confidencialidad o de no divulgación.....	43
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	43
12.1 Requisitos de seguridad de los sistemas de información	43
12.1.1 Análisis y especificación de los requisitos de seguridad.	43
12.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	44
12.1.3 Protección de las transacciones por redes telemáticas	44
12.2 Seguridad en los procesos de desarrollo y soporte	44
12.2.1 Política de desarrollo seguro de software	44
12.2.2 Procedimientos de Control de cambios en los sistemas	44
12.2.3 Revisión técnica de las aplicaciones después de efectuar cambios en los sistemas operativos	44
12.2.4 Restricciones a los cambios en los paquetes de software	44
12.2.5 Uso de principios de ingeniería en protección de sistemas.....	45
12.2.6 Entorno de desarrollo seguro	45
12.2.7 Desarrollo tercerizado	45
12.2.8 Pruebas de funcionalidad durante el desarrollo de los Sistemas	45
12.2.9 Pruebas de aceptación del sistema	45

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 6 de 54

12.3 Los datos de prueba	45
12.3.1 Protección de los datos de prueba	45
13. RELACIONES CON LOS PROVEEDORES	46
13.1 Seguridad de la información en relación con los proveedores	46
13.1.1 Política de seguridad de la información para las relaciones con proveedores	46
13.1.2 Tratamiento del riesgo dentro de acuerdos con proveedores	46
13.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	46
13.2 Gestión de la prestación de servicios por proveedores	46
13.2.1 Seguimiento y revisión de los servicios de proveedores	47
13.2.2 Gestión de cambios en los servicios prestados por proveedores	47
14. GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN	47
14.1 Gestión de incidentes de seguridad de la información y mejoras	47
14.1.1 Responsabilidades y procedimientos	48
14.1.2 Informar sobre los eventos de seguridad de información	48
14.1.3 Notificación de puntos débiles de la seguridad	48
14.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	48
14.1.5 Respuesta a incidentes de seguridad de la información	48
14.1.6 Aprendizaje de los incidentes de seguridad de la información	48
14.1.7 Recopilación de evidencias	48
15. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	49
15.1 Continuidad de la seguridad de la Información	49
15.1.1 Planificación de la continuidad de la seguridad de la información y Análisis de riesgos	50
15.1.2 Implantación de la continuidad de la seguridad de la información	51
15.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	51
15.2 Redundancias	51
15.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	51
16. CUMPLIMIENTO	52
16.1 Cumplimiento de los requisitos legales y contractuales	52
16.1.1 Identificación de la legislación aplicable y los requisitos contractuales	53
16.1.2 Derechos de propiedad intelectual	53
16.1.3 Protección de los registros	53
16.1.4 Protección de datos y privacidad de la información personal	53
16.1.5 Regulación de los controles criptográficos	53

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 7 de 54

16.2 Revisiones de la seguridad de la información.....	53
16.2.1 Revisión independiente de la seguridad de la información	53
16.2.2 Cumplimiento de las políticas y normas de seguridad	54
16.2.3 Comprobación del cumplimiento.....	54

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 8 de 54

1. INTRODUCCIÓN

La Política del sistema de Gestión de Seguridad de la Información es la declaración general que representa la posición de la administración de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, con respecto a la protección de los activos de información (los datos y la información en si misma, los funcionarios, contratistas, terceros, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y que son cubiertos con la implementación del Sistema de Gestión de Seguridad de la Información por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la entidad.
- Garantizar la continuidad del negocio frente a incidentes.

Con esta política se busca identificar, evaluar, gestionar y minimizar cualquier tipo de riesgo relacionado con seguridad, asociados a amenazas que atenten en contra de la confidencialidad, integridad y disponibilidad de la información en cada uno de los procedimientos que se tienen en la Entidad.

1.1 Objetivo

El Fin de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 9 de 54

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información, según se define en el Documento del Alcance del SGSI.

Los usuarios de este documento son todos los funcionarios de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, como también terceros externos a la Entidad.

Este documento describe el uso adecuado de activos de información, incluyendo a los servicios, aplicativos, equipos de cómputo y la plataforma tecnológica Institucional.

1.2 Documentos de Referencia

A continuación, se relacionan los principales documentos de referencia para las políticas de seguridad de la información de la Institución.

- Norma ISO/IEC 27001:2013
- Documento sobre el alcance del SGSI
- Análisis de Riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales

1.3 Términos y definiciones

Confidencialidad: característica de la información que está disponible solo para personas o sistemas autorizados.

Integridad: característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Activo de información: Un activo en relación a la presente política de seguridad de la información, se refiere a cualquier dato, información o sistema relacionado con el tratamiento de la misma que tenga valor para la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, incluyendo bases de datos, documentación, manuales, software, hardware, contratos de equipo de comunicaciones, servicios informáticos y de comunicaciones y dispositivos del Internet de las cosas como Cámaras IP, DVRs, actuadores y sensores como también a las personas, quienes los

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 10 de 54

generan, transmiten y destruyen información. Todos los activos deberán estar claramente identificados manteniendo un inventario con los más importantes.

Seguridad de la información: Es el conjunto de medidas preventivas y correctivas para proteger la información manteniendo la confidencialidad, disponibilidad e integridad de la misma.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Malware: Son programas maliciosos creados para infectar/ comprometer sistemas informáticos alterando su funcionamiento y facilitando el compromiso de los activos de información digital.

1.4 Alcance y aplicabilidad

La presente Política de Seguridad de la Información se aplica a todos los activos de información institucional, activos de información externos de clientes, y de terceros que brinden servicios a la institución, en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA

Las Políticas de Seguridad de la Información contenidas en este documento, son mandatos generales, de obligatorio cumplimiento por todos los funcionarios, contratistas y terceras partes, que presten sus servicios a la Entidad.

1.5 Nivel de Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

1.6 Estructura del documento de políticas de seguridad

Este documento de política se divide en dos partes, y guarda la siguiente estructura:

- Dos (2) capítulos introductorios, con los términos generales y el establecimiento de la evaluación y el tratamiento de los riesgos.
- Catorce (14) dominios, 35 objetivos de control y 114 controles de acuerdo a lo estipulado en la norma ISO27000 Versión 2013.

1.7 Políticas Específicas de Seguridad de la Información Anexos

Las principales políticas específicas referentes a la seguridad de la información se encuentran como documentos anexos y se listan a continuación:

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 11 de 54

- Política de Acceso
- Política de Autenticación
- Política de Uso Aceptable
- Política de Privacidad
- Política de Evaluación de Adquisiciones
- Política de Mantenimientos

2 GESTIÓN Y TRATAMIENTO DE ACTIVOS DE INFORMACIÓN

2.1 Principal concepto de activos de información

Los activos de información son el activo más importante de toda la Entidad y están representados por colecciones de datos que se consideran la materia prima de los procesos de toda Entidad, también se consideran activos de información a los flujos de información resultantes del procesamiento incluyendo directorios y archivos digitales en cualquier formato. De la misma forma se incluyen a los sistemas de información, infraestructura tecnológica e información impresa y en cualquier tipo de formato físico.

Los activos de información se clasifican de acuerdo al nivel de importancia que representen para la Entidad; esta clasificación también permite determinar el grado de protección que debe brindarse a cada activo de información. Por lo anterior la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe definir los controles para salvaguardar la información creada, procesada, transmitida y/o almacenada resultado de sus procesos internos, con el fin de minimizar los impactos financieros, operativos y/o legales debido a la exposición y/o uso incorrecto de la misma.

Los activos de Información que la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA utilice para el desarrollo de sus objetivos debe tener asignado un responsable, quién la utiliza y es el que responde por su correcto tratamiento al igual que un custodio. Así, él toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de tratamiento.

Cada responsable de los activos de información debe salvaguardar y vigilar su correcto tratamiento, los lugares donde reside y los usuarios de la misma. Dichos usuarios deben demostrar una necesidad en sus funciones para su acceso, el cual debe ser vigilado por el responsable. La Información provista por los clientes, proveedores, terceros, y funcionarios es privada y su tratamiento dentro de las premisas de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA está enmarcado para los fines que fue obtenida.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 12 de 54

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA provee los medios necesarios para asegurarse de que cada Usuario preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer o sobrepasar cualquier control de Seguridad de la Información en forma no autorizada será sujeto de las acciones legales correspondientes.

Los recursos de Información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA son exclusivamente para propósitos de la Entidad y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA promueve el buen uso de los recursos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data, y la protección de los datos de sus propietarios.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, se reserva el derecho de restringir el acceso a cualquier Información en el momento que lo considere conveniente.

2.2 Incidente de seguridad

Se deberá notificar al proceso de Gestión Administrativa y tecnológica:

- En caso de que se presente un evento adverso en la computadora asignada, o en la red de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.
- Cuando exista la sospecha o el conocimiento de que información confidencial o privada ha sido revelada, modificada, alterada o borrada sin la autorización.
 - Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

El proceso de Gestión Administrativa y tecnológica, tiene establecidas las responsabilidades y procedimientos que aseguren una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información que se llegasen a presentar en la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 13 de 54

3 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA consciente de la importancia de la seguridad de la información dentro de los procesos gerenciales, administrativos, operativos y académicos; y comprometida con la calidad de los servicios ofertados y la satisfacción de los funcionarios, contratistas y ciudadanos, asume un compromiso expreso de protección de sus activos como parte de la estrategia de continuidad del negocio, administración de riesgos y la consolidación de una cultura de seguridad de la información.

Consecuente con las necesidades referentes a la seguridad de la información, la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA implementa un modelo de gestión de seguridad de la información como herramienta para identificar y minimizar los riesgos a los que se expone la información tratada en todos sus procesos de negocios, al tiempo que establece una cultura de seguridad, facilita la reducción de costos operativos y financieros a la vez que garantiza el cumplimiento de los requerimientos contractuales, regulatorios y legales vigentes.

La Entidad tiene claro que el proceso de análisis de riesgos es el soporte para el desarrollo de las políticas de seguridad de la información, de los controles y de los objetivos de control seleccionados para obtener los niveles de protección esperados. El proceso de análisis de riesgos será liderado de manera permanente por el Oficial de Seguridad de la información.

Esta política será revisada con regularidad, cuando ocurran cambios en los procesos del negocio, en su estructura, en sus objetivos o como parte del proceso de revisión gerencial con el fin de asegurar que esta siga siendo adecuada y este ajustada a los requerimientos identificados.

3.1 Directrices de la Dirección en seguridad de la información.

Objetivo: Dar las directrices para la entidad en lo relacionado con Seguridad de la Información.

3.1.1 Conjunto de políticas para la seguridad de la información

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA se compromete a producir, proveer y divulgar información y conocimiento confiable y oportuno preservando la confidencialidad, integridad y disponibilidad de la

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 14 de 54

información misional de acuerdo a las disposiciones legales y técnicas y a las responsabilidades adquiridas para la satisfacción de los clientes y la protección de la información contra amenazas internas y externas, mediante la implementación de buenas prácticas en la gestión de riesgos, el fortalecimiento de la capacidad institucional y la operación bajo un sistema de gestión integrado que mejore continuamente su eficacia, eficiencia y efectividad.

3.1.2 Revisión de las políticas de seguridad de la información.

Las políticas de seguridad de la información se revisarán periódicamente (mínimo una vez por año), o antes, en caso de producirse cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc., que puedan afectar su continuidad. La aprobación de las actualizaciones y/o modificaciones, se realizará por parte del Comité de Seguridad de la Información.

4. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la Entidad.

4.1 Entidad interna

Oficial de Seguridad de la Información

La entidad cuenta con un profesional especializado quien desarrolla las funciones de oficial de seguridad de la información.

El Oficial de Seguridad de la Información - de Seguridad tiene toda la responsabilidad máxima respecto a seguridad de la información.

Comité de Seguridad de la Información.

El Comité de MIPG cumple con las funciones del comité de Seguridad de la Información, como un cuerpo integrado por el oficial de Seguridad de la información, representantes de los procesos de: Servicio al Ciudadano, Gestión Documental, Gestión Administrativa y tecnológica, Gestión Financiera, Gestión Jurídica, Gestión de Talento Humano de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA y su objetivo es: “Asegurar que exista dirección y apoyo gerencial para establecer, implementar y monitorear las estrategias de Seguridad de la Información que requiera la entidad”. La actualización y mantenimiento de las políticas de seguridad de la información será realizado por el Oficial de Seguridad – **OSI**, junto con el Comité de Seguridad de la Información — **CSI**, Responsable de Seguridad de los activos de Información de la institución.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 15 de 54

El Oficial de Seguridad de la Información tiene dentro de sus responsabilidades la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a las diferentes dependencias de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA que así lo requieran.

Dentro de la Entidad interna de Seguridad de la Información se identificarán los siguientes roles: Custodio, Propietario o Usuario de la información; cada rol debe identificar, analizar, evaluar, tratar y monitorear el cumplimiento de la Política.

Custodio: Tienen la responsabilidad de administrar el activo, monitorearlo y hacer efectivas las medidas de protección definidas para este.

Propietario o Usuario: Debe verificar la integridad de la información y velar por que se mantenga la disponibilidad y confidencialidad de la misma.

4.1.1 Asignación de responsabilidades para la seguridad de la información.

Las responsabilidades de seguridad de la información están definidas y asignadas de acuerdo a la clasificación dada a la información.

4.1.2 Segregación de las tareas

La responsabilidad de la información deberá estar en cabeza de una sola persona para evitar conflicto en cuanto a responsabilidades. Lo anterior permite reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de la Entidad.

4.1.3 Contacto con las autoridades

Se mantendrán los contactos apropiados con las autoridades pertinentes (CoCERT, Unidad de Delitos Informáticos de la Fiscalía General de la Nación, Policía, Bomberos, Defensa Civil), en caso de encontrar violación a la presente política de seguridad de la información.

4.1.4 Contacto con grupos de interés especial

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA mantendrá los contactos apropiados con los grupos de interés especializados en seguridad de la información tales como CSIRT Contacto equipo de respuesta a incidentes de seguridad informática, como también tendrá participación en foros de seguridad especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 16 de 54

4.1.5 Seguridad de la información en la gestión de proyectos

La seguridad de la información se dirigirá en la gestión de proyectos y se deberá cumplir, independientemente del tipo de proyecto.

4.2 Dispositivos para movilidad y el teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

4.2.1 Política de uso de dispositivos para movilidad

El uso de los equipos portátiles fuera de las instalaciones de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA únicamente se permitirá a usuarios autorizados por el proceso de Gestión Administrativa y tecnológica, previa solicitud de la dependencia respectiva, y éstos se protegerán mediante el uso de los siguientes controles tecnológicos:

- Antimalware actualizado.
- Cifrado de datos.
- Ejecución de Backups.
- Restricción en la ejecución de aplicaciones.
- Restricción de conexión de dispositivos USB.
- Protección física mediante la guaya de seguridad.

La sincronización de dispositivos móviles con cualquier sistema de información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, sólo estará permitido para personal autorizado por el proceso de Gestión Administrativa y tecnológica y la dependencia respectiva.

4.2.2 Teletrabajo

Cualquier funcionario de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, autorizado por el proceso de Gestión Administrativa y tecnológica, que requiera tener acceso a la información de la Institución desde redes externas, podrá acceder remotamente mediante un proceso de autenticación; uso de conexiones seguras. Lo anterior asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 17 de 54

5. SEGURIDAD DE LOS RECURSOS HUMANOS

5.1 Antes de la contratación

Objetivo: Asegurar que los funcionarios y contratistas entiendan sus responsabilidades y que estas son adecuadas para las funciones que realizan.

5.1.1 Investigación de antecedentes

Se debe realizar la verificación de antecedentes judiciales, disciplinarios, fiscales y seguimiento a la hoja de vida de todos los candidatos a emplear de conformidad con el reglamento interno de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA y las leyes y regulaciones del estado colombiano.

5.1.2 Términos y condiciones de contratación

Los acuerdos contractuales con los funcionarios y los contratistas deberán establecer las responsabilidades establecidas por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA en el cumplimiento del acuerdo de confidencialidad y de la presente Política de Seguridad de la Información.

5.2 Durante la contratación y/o empleo

Objetivo: Asegurar que los funcionarios y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.

La capacitación en Seguridad de la Información es obligatoria para todo el personal que ingrese vinculado de manera temporal y/o indefinida a la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA. Se deberá asistir de manera obligatoria durante su inducción, a las charlas que sobre los requerimientos de Seguridad de la Información se dicten.

El proceso de Gestión Administrativa y tecnológica, de acuerdo a la estructura orgánica de la entidad, es el único responsable de asignar, administrar y reasignar la infraestructura tecnológica independientemente del origen de los recursos económicos y del ordenador del gasto.

5.2.1 Responsabilidades de gestión

La administración pedirá a todos los funcionarios y contratistas, aplicar todos los lineamientos referentes a la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA. Todos los funcionarios y contratistas tendrán acceso permanente a la política y se obligan a cumplirla.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 18 de 54

El personal que ingrese vinculado de manera temporal y/o indefinida a la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, deberá firmar que conoce y acepta lo definido en la política de Seguridad.

5.2.2 Concientización, educación y formación en la seguridad de la información

El proceso de Gestión Administrativa y tecnológica realizará capacitaciones periódicas a lo largo del año, a todos los funcionarios y contratistas de la Entidad de sensibilización, educación y formación adecuada y actualizaciones periódicas en las políticas y procedimientos de la Entidad, que sea relevante para su función laboral.

5.2.3 Proceso disciplinario

Se solicitará proceso disciplinario formal y comunicado en contra de los funcionarios que hayan cometido una violación de la seguridad de la información, y según corresponda la investigación será tramitada por el Proceso de Control Interno Disciplinario de la Entidad o la Procuraduría General de la Nación.

5.3 Terminación o cambio de empleo

Objetivo: Proteger los intereses de la Entidad como parte del proceso de terminación o cambio el empleo.

5.3.1 Terminación o cambio de puesto de trabajo

Las responsabilidades de seguridad de la Información y deberes que siguen vigentes después de la terminación o cambio de empleo, se deben definir y comunicarse al empleado o contratista y se deben hacer cumplir.

Es responsabilidad de la oficina de Gestión de Talento Humano y del proceso de Gestión Administrativa y tecnológica asegurar que en el evento de la terminación y/o cambio de cargo al interior de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, el empleado haga la devolución de todos los activos de información y elementos asignados durante su relación.

La vigencia de los derechos de acceso y su revocatoria, debe estar estrechamente relacionados con la terminación de la relación laboral y/o contractual del funcionario y/o cambio del rol del funcionario en la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 19 de 54

6. GESTIÓN DE ACTIVOS

6.1 Responsabilidad sobre los activos

Objetivo: Identificar los activos de la Entidad y definir las responsabilidades de protección adecuados.

Todos los activos de información en la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA serán clasificados según el contenido, y los controles adecuados serán implementados de acuerdo a su importancia en la Entidad.

6.1.1 Inventario de activos

Los activos relacionados con la información y las instalaciones de procesamiento de información deben ser identificados dentro del inventario de activos de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

6.1.2 Propiedad de los activos

Los activos mantenidos en el inventario son de propiedad de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

6.1.3 Uso aceptable de los activos

Las normas para el uso aceptable de la información y de los activos asociados a la información y las instalaciones de procesamiento de información están identificadas en el presente documento deben cumplirse de forma obligatoria por sus responsables.

6.1.4 Devolución de los activos

Todos los funcionarios y contratistas deberán devolver todos los activos de la Entidad en su poder a la terminación de su empleo, contrato o acuerdo.

6.2 Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel adecuado de protección, de acuerdo con su importancia para la Entidad.

6.2.1 Directrices de clasificación

La información se clasificará en función de su criticidad, valor para la Entidad y carácter de confidencialidad.

Todos los activos de información en la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA serán clasificados según el contenido y los controles adecuados serán implementados de acuerdo a su importancia en la Entidad. Esta

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 20 de 54

clasificación será realizada por el responsable de la misma, basado en el procedimiento de identificación y clasificación de activos de la institución; teniendo en cuenta, además: los requerimientos legales de retención.

Estos niveles serán divulgados y oficializados a los Usuarios de la Información para asegurar que los niveles de protección son entendidos y se mantienen a través de la Entidad.

La información clasificada tendrá un conjunto de controles determinados por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, los que podrán ser complementados y aumentados, nunca disminuidos por el responsable de la Información, el Oficial de Seguridad y/o el Comité de Seguridad de Información de la institución con apoyo del proceso de Gestión Administrativa y tecnológica. Dichos controles se utilizan para proveer un nivel de protección de la Información apropiado y consistente dentro de la Entidad, sin importar el medio, formato o lugar donde se encuentre. Estos controles se aplican y mantienen durante el ciclo de vida de la Información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

Si la información clasificada de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe ser entregada a contratistas y terceros, previamente se deben firmar los acuerdos de confidencialidad respectivos, que incluyan el seguimiento y cumplimiento de las prácticas de gestión segura de la Información al tenor de lo establecido en la Política. Igualmente, si la Información clasificada de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA es requerida por algún ente externo o ciudadano en donde opere la Entidad, su entrega está supeditada a la aprobación previa de su responsable y de las instancias establecidas.

Los activos de información de la Entidad, se clasificarán de acuerdo a los niveles que se relacionan a continuación:

Datos e información pública: Aquellos en los que la Ley no ha dado el carácter de reservado y su divulgación y/o conocimiento por parte de personal externo no representa ningún riesgo.

Datos e información privada: Aquellos en los que la Ley ha otorgado el carácter de reservados y de protección legal, que no puede ser publicada y que su exposición podría representar un riesgo significativo para la institución.

Datos e información Confidencial: Datos e información que no es de dominio público y que su exposición puede ocasionar pérdidas graves que representen un riesgo mayor para la Entidad. Como también información que ha sido obtenida u ofrecida por orden de una

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 21 de 54

autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de administración de datos personales.

Acceso a información Confidencial.

- Las terceras partes que requieran acceso a esta información en medio físico y/o electrónico, deben presentar a la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA una autorización por parte del dueño de la información y se debe firmar un acuerdo de confidencialidad indicando las restricciones de uso de dicha información.
- Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación.
- Los servidores públicos, contratistas, pasantes o estudiantes no pueden tomar información confidencial cuando termine su vínculo con la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

La destrucción de información Confidencial.

La destrucción de este tipo de información será realizada de acuerdo a métodos aprobados por el responsable de seguridad de la información (Oficial de Seguridad y/o Comité de Seguridad de la información). El único impedimento para la destrucción de la información puede ser una restricción señalada expresamente por parte de la Oficina Gestión Jurídica, de acuerdo a la estructura orgánica de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, y/o radicada en las tablas de retención documental.

Almacenamiento de Información.

La información confidencial almacenada en cualquier medio electrónico, o físico, debe ser protegida por medio de mecanismos de cifrado.

Los equipos de cómputo y/o portátiles que almacenen información confidencial deben estar protegidos con mecanismos de control de acceso para evitar que ante la pérdida del equipo una persona no autorizada pueda consultar, manipular o eliminar a la información allí almacenada. Así mismo si son reasignados a usuarios diferentes, se debe borrar la información del disco de forma segura, de acuerdo a los lineamientos dados por el responsable de seguridad de la información (Oficial de Seguridad y/o Comité de Seguridad de la información).

Impresión de información. La información clasificada como confidencial debe ser enviada a la impresora y recogida inmediatamente, evitando que personal no autorizado tenga acceso a ésta.

Divulgación de información a terceros.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 22 de 54

Los funcionarios no deben divulgar información a terceros acerca de las vulnerabilidades de los sistemas lógicos o físicos de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, sin la previa autorización por parte de los responsables de Seguridad de la Información y la firma de un acuerdo de confidencialidad.

6.2.2 Etiquetado y manipulado de la información

Los procedimientos para el etiquetado de la información serán aplicados de acuerdo con el esquema de clasificación de la información aprobada por la entidad, lo anterior teniendo en cuenta las tablas de Retención Documental aprobadas para las diferentes áreas.

6.2.3 Manipulación de activos

Se aplicarán los procedimientos para el manejo de los activos de conformidad con el esquema de clasificación de la información aprobada por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA y presentada en este documento.

6.3 Manejo de los soportes de almacenamiento

Objetivo: Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación.

6.3.1 Gestión de soportes extraíbles

La gestión de medios extraíbles se realizará de acuerdo con el esquema de clasificación adoptado por la entidad.

Los equipos de cómputo que tienen autorizado el manejo de USB y unidades reproductoras de CD/DVD, deben cumplir los siguientes requisitos.

- Tener habilitado el escaneo automático de malware
- Tener configurada en la herramienta antimalware, el bloqueo de la reproducción automática de archivos ejecutables

6.3.2 Eliminación de soportes.

La información será eliminada de los medios de comunicación de forma segura cuando ya no sea necesaria, utilizando procedimientos formales.

6.3.3 Soportes físicos en tránsito

Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte, esto con la utilización de bolsas de seguridad y de técnicas de cifrado de datos.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 23 de 54

Se debe implementar la utilización de protocolos de seguridad para la encriptación de las claves más sofisticadas.

7. CONTROL DE ACCESO

7.1 Requisitos de negocio para el Control de acceso

Objetivo: Limitar el acceso a las instalaciones de procesamiento de la información y de la información.

7.1.1 Política de Control de acceso

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA garantiza entornos con controles de acceso idóneos, los cuales aseguran el perímetro, tanto en oficinas, recintos, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos. Del mismo modo, controla las amenazas físicas externas y vela por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información documentales.

Así mismo, exige a los proveedores de servicios de tecnología, el cumplimiento de la implantación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con que éste debe contar.

Los funcionarios responsables de las áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- Las áreas de administrativas se catalogan como seguras y deben permanecer cerradas y custodiadas
- El acceso a áreas seguras donde se procesa o almacena información privada y confidencial, está limitado únicamente a personas autorizadas.

El acceso a áreas seguras requiere esquemas de control de acceso, como tarjetas, llaves o candados.

- El responsable de un área segura debe asegurar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras, salvo se tenga una autorización expresa del Comité de Seguridad de la Información – CSI.
- Se utilizan bitácoras para registrar la entrada y salida del personal.
- Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 24 de 54

7.1.2 Control de acceso a las redes y servicios asociados

Los usuarios que dispongan de acceso y servicios de la red son los que han sido específicamente autorizados para su uso.

Cada usuario es responsable por sus acciones mientras usa cualquier recurso de Información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA. Por lo tanto, la identidad de cada Usuario de los recursos de información está establecida de una manera única. Esta identidad de ninguna manera o por ninguna circunstancia podrá ser compartida, en caso tal que se evidencie lo anterior este será tratado como una infracción a la seguridad de la información.

Los niveles de acceso deben reflejar permanentemente una necesidad clara y demostrada de funciones y no deben comprometer la segregación de funciones y responsabilidades.

7.2 Gestión de acceso de usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados para evitar el ingreso no permitido a los sistemas y servicios.

7.2.1 Gestión de altas y bajas en el registro de usuarios

Se llevará a cabo un proceso formal de registro y anulación de usuario para permitir la asignación de derechos de acceso.

La eliminación de un identificador de usuario debe ser realizada inmediatamente haya finalizado su relación contractual del usuario con la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

7.2.2 Gestión de los derechos de acceso asignados a los usuarios.

El acceso a la información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, es otorgado sólo a Usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad o tipo de servicio. El acceso a los recursos de información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, es restringido en todos los casos sin excepción, y se da específicamente a quienes lo requieran en razón de sus funciones, con los privilegios apropiados y por un tiempo limitado.

Se debe identificar y autenticar a cualquier usuario que de manera local o remota, requiera utilizar los Recursos de Tecnología y operación de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, para lo que se requiere contar con sistemas de seguridad que cumplan con las siguientes características:

Debe estar activo para acceder a la plataforma tecnológica y de operación de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 25 de 54

CATALINA, lo que significa que cada usuario tiene que identificarse y autenticarse antes de acceder a un recurso de tecnología por medio de un usuario y una contraseña.

- Una vez se han identificado y autenticado, los usuarios sólo podrán acceder a los recursos sobre los cuales están autorizados.
- Los eventos de ingreso y autenticación de usuarios serán registrados y monitoreados por los responsables de la información.

Los usuarios deben cumplir prácticas como las recomendadas en el Anexo para la selección y uso de las contraseñas.

El acceso a los Activos de Información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, debe ser controlado mediante un proceso formal de creación, modificación y eliminación del identificador de usuario.

Únicamente el responsable de la información, puede autorizar la creación de un usuario, este identificador de usuario debe ser asociado sólo a un individuo y la solicitud debe obedecer a una razón legítima de la Entidad.

El uso remoto de los activos de información y la computación móvil será realizado bajo una autorización previa de los responsables de la información, junto con su respectivo manejo de riesgo aprobado por La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

Ningún rol puede tener acceso a más de un ambiente

7.2.3 Gestión de derechos de acceso privilegios especiales

La asignación y utilización de los derechos de acceso preferente se deberá restringir y controlar.

El uso de las credenciales/contraseñas de usuarios administradores de los diferentes sistemas y plataformas, tales como: “root”, “adm”, “administrador”, “manager” y “system”, entre otros, deben ser controlados solamente por el personal encargado del proceso de Gestión Administrativa y tecnológica y deben ser tratados como información confidencial.

7.2.4 Gestión de información confidencial de autenticación de los usuarios

La asignación de la información secreta de autenticación como usuarios y contraseñas deben controlarse a través de un proceso de gestión formal y de acuerdo a la clasificación dada a los activos por parte de los responsables; por lo que deben transmitirse y almacenarse de forma cifrada.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 26 de 54

7.2.5 Revisión de los derechos de acceso de los usuarios

Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares. Cualquier desviación será tratada como un incidente en seguridad de la información.

Los responsables deben dejar trazas del ejercicio de esta actividad, las que serán objeto de revisiones de parte de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

7.2.6 Retirada o adaptación de los derechos de acceso

Los derechos de acceso de todos los funcionarios y/o contratistas de la información e instalaciones de informática serán retirados en el momento de retiro de su empleo y/o terminación de contrato.

7.3 Responsabilidades de los usuarios

Objetivo: Hacer que los usuarios responsables de salvaguardar su información se autentiquen.

7.3.1 Uso de la información confidencial para la autenticación

Se exigirá a los usuarios que sigan prácticas de la Entidad en el uso y manejo de complejidad de la información secreta de autenticación.

7.4 Control de acceso a sistemas y aplicaciones

Objetivo: Evitar el acceso no autorizado a los sistemas y aplicaciones.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA tiene establecidos controles físicos y de acceso lógico para los ambientes de desarrollo, pruebas y producción de los Activos de Información para que permanezcan completamente separados.

El acceso a la información en producción de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe hacerse únicamente por los aplicativos y sistemas autorizados. En ningún caso la información puede ser accedida directamente.

Si entes externos tienen acceso a información crítica de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA se deben suscribir acuerdos para la salvaguarda de la información. La información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA que está en manos de personas externas debe tener el mismo o mayor nivel de protección como si estuviera administrada por la institución, por lo cual es necesario efectuar revisiones a fin de conocer cómo se está manejando y protegiendo la información externamente.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 27 de 54

7.4.1 Restricción del acceso a la información

El acceso a la información estará restringido de conformidad con la política de Control de acceso.

7.4.2 Procedimientos seguros de inicio de sesión.

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro.

7.4.3 Sistema de gestión de contraseñas

Todo funcionario, recibirá las credenciales de acceso compuestas por un nombre de usuario y una contraseña, con las cuales podrá acceder a los recursos informáticos de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, la cual es de cambio obligatorio en el primer uso garantizando así su responsabilidad y único conocimiento sobre la misma. Dicha contraseña debe tener una longitud mínima de 8 caracteres alfanuméricos, diferentes a nombres propios, números de cedula, números de placa de vehículos, fecha de nacimiento o cualquier otra palabra de fácil identificación.

Por seguridad se recomienda el cambio de dichas claves con una periodicidad de 30 (treinta) días.

Después de 3 (tres) intentos no exitosos de digitar la contraseña la cuenta de usuario será bloqueado de manera inmediata y deberá solicitar el desbloqueo al proceso de Gestión Administrativa y tecnológica.

Se prohíbe el uso de contraseñas compartidas. La contraseña es personal e intransferible. Las contraseñas nunca serán modificadas telefónicamente o vía email.

7.4.4 Uso de herramientas de administración de sistemas

El uso de productos de software y demás utilitarios que podrían ser utilizados para eludir o afectar los controles de acceso serán de uso restringido para el personal asignado por el Comité de Seguridad de la Información - CSI y serán de uso controlado solo para situaciones que por necesidad del servicio lo ameriten.

7.4.5 Control de acceso al código fuente de los programas

El acceso al código fuente de los productos de software es limitado. Solamente el personal de desarrollo de software del proceso de Gestión Administrativa y tecnológica tendrá acceso otorgado a esta información y tendrán autorización de uso de la misma. Se debe contar con una bitácora de registro de acceso a las librerías de código fuente.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 28 de 54

8. CIFRADO

8.1 Controles criptográficos

Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

8.1.1 Política sobre el uso de controles criptográficos

Se deben utilizar controles criptográficos en los siguientes casos:

- En la protección de llaves, contraseñas y claves de acceso a sistemas computacionales, datos y servicios.
- En la transmisión de información Confidencial a través de cualquier medio tecnológico.
- Para el resguardo y almacenamiento de la información confidencial.

Con respecto a los algoritmos de cifrado que debe usarse para la protección de los activos de información digitales:

- Se hará uso de algoritmos criptográficos considerados como estándares internacionales.
- Se Utilizará criptografía Simétrica para cifrar los activos de información digitales.
- Se utilizará criptografía Asimétrica para el intercambio y gestión de las llaves criptográficas.

8.1.2 Administración de llaves

La política sobre uso, protección y duración de las llaves criptográficas se realiza durante todo su ciclo de vida según el procedimiento de gestión de llaves criptográficas anexo a este documento.

9. LA SEGURIDAD FÍSICA Y AMBIENTAL

9.1 Áreas seguras

Objetivo: Evitar el acceso físico no autorizado, daños e interferencia para la información de la Entidad y las instalaciones de procesamiento de información.

9.1.1 Perímetro de seguridad física

Los límites físicos de las áreas que contienen a los activos de información deben contar con los controles necesarios para evitar tanto el acceso no autorizado como la exposición de la confidencialidad, integridad y disponibilidad de estos activos.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 29 de 54

9.1.2 Controles físicos de entradas

Las áreas seguras se protegerán mediante controles de acceso físicos adecuados para garantizar que se le permita la entrada únicamente al personal autorizado.

Para el ingreso de terceros al Data Center, se tienen que registrar en la bitácora ubicada en un lugar visible a la entrada a este lugar.

Los privilegios (de los funcionarios y/o contratistas) de acceso físico al Data Center deben ser eliminados o modificados oportunamente a la terminación, transferencia o cambio en las labores de un funcionario autorizado.

Las oficinas e instalaciones donde se realice atención al público no deben permanecer abiertas cuando los funcionarios se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.

En caso de que el funcionario deba levantarse del puesto, este debe bloquear la estación de trabajo o equipo de cómputo, de igual manera deben tener habilitado el protector de pantalla con contraseña.

Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizadas por los funcionarios y/o contratistas autorizados y salvo situaciones de emergencia, estos no deben ser transferidos a otros funcionarios de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA o funcionarios provistos por terceras partes.

Las oficinas e instalaciones donde se maneje información sensible deben contar con sistemas de alarmas y cámaras.

Todos los funcionarios deben permanecer con el carnet que los identifica como funcionarios y/o contratistas de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, mientras permanezcan en las instalaciones.

Todos los funcionarios deben reportar, a la mayor brevedad, cualquier sospecha de pérdida o robo de carnet de identificación y tarjetas de acceso físico a las instalaciones de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA

Los funcionarios de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA no deben intentar ingresar a áreas a las cuales no tengan la debida autorización.

Todos los visitantes que ingresan a la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, deben ser recibidos y estar acompañados por la persona a quien visitan durante su permanencia en las instalaciones del mismo.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 30 de 54

Todos los visitantes que ingresan a la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, deben ser registrados en bitácora de visitantes con los datos personales y hora de entrada y salida de las instalaciones.

La documentación física generada, recibida y, en general, manipulada por los funcionarios de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA y los funcionarios provistos por terceras partes debe estar ubicada en archivos o repositorios con condiciones de temperatura y humedad adecuadas, de acuerdo con las directrices de la función archivística de la institución.

9.1.3 Seguridad de oficinas, despachos, salas e instalaciones

Las oficinas, despachos, salas y demás instalaciones en donde se procese información deben contar con mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y gabinetes con llaves para la disposición de documentos sensibles.

El ingreso de terceros a las oficinas, despachos, salas y demás instalaciones de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe estar debidamente registrado mediante una bitácora a la entrada de estos lugares. El ingreso a estos lugares debe ser monitoreado regularmente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

El Data Center debe estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.

Deben existir mecanismos de revisión y control del ingreso de cualquier tipo de material al Data Center.

Se debe monitorear y revisar de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte del Data Center, como son el sistema de aire acondicionado y el sistema de detección y extinción de incendios, entre otros.

Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, deben ser realizados por personal especialista y debidamente autorizado e identificado.

Se deben realizar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y/o plantas eléctricas, de los sistemas de detección y extinción de incendios y del sistema de aire acondicionado.

Se deben realizar mantenimientos preventivos y correctivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 31 de 54

Se debe proveer un procedimiento, que garantice la realización del mantenimiento preventivo y correctivo de las estaciones de trabajo y equipos portátiles, así como su adecuación para la reutilización o reasignación de manera segura en el cual se conserve la disponibilidad, integridad y confidencialidad de la información contenida en los mismos.

El proceso de Gestión Administrativa y tecnológica debe garantizar la adopción de los controles necesarios para asegurar que los suministros de electricidad, así como las redes de comunicaciones se encuentran protegidos.

9.1.4 Protección contra las amenazas externas y ambientales

El proceso de Gestión Administrativa y tecnológica y el Comité de Seguridad de la información deben monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos.

En el Data Center deberán existir sistemas de detección y extinción automáticas de incendios e inundación y alarmas en caso de detectarse condiciones inapropiadas.

Los niveles de temperatura y humedad relativa en el Data Center deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado.

9.1.5 Trabajar en áreas seguras

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA a través del responsable de seguridad de información, debe establecer controles ante las diferentes amenazas que pueden afectar la normal operación. Los controles a implementar son:

Medio ambiente: El proceso de Gestión Administrativa y tecnológica y el Comité de Seguridad de la información deberán monitorear las variables de temperatura y humedad de las áreas de procesamiento de información.

Identificación de terceros, explosivos y corrosivos: Todos los visitantes o terceras personas, que ingresan a las instalaciones de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, deben poseer una identificación a la vista. Por ninguna razón se podrá tener material explosivo o corrosivo dentro o en sitio cercano a áreas definidas como seguras.

Fuego: En los centros de procesamiento deben instalarse detectores de humo, en forma adecuada y en número suficiente, para detectar conato o indicio de incendios. En las áreas seguras no se debe tener material inflamable tales como: Cajas, manuales, formas continuas, papel.

Los detectores deben probarse de acuerdo a las recomendaciones del fabricante o al menos una vez cada seis meses.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 32 de 54

Se deben tener extintores debidamente provisionados, con carga vigente y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.

Interferencia eléctrica y/o radiación electromagnética: El cableado lógico, debe estar protegido de las interferencias electromagnéticas producidas por equipos eléctricos y/o industriales.

Los cables de potencia deben estar separados de los cables de comunicación, siguiendo normas técnicas. Los equipos deben protegerse de fallas de potencia u otras anomalías de tipo eléctrico.

Sistema de abastecimiento de Potencia: El correcto uso de las UPS, se debe probar según las recomendaciones del fabricante, de tal forma que se garantice su operación y el suficiente tiempo para realizar las funciones de respaldo servidores y aplicaciones.

La planta eléctrica debe probarse regularmente, de acuerdo a las recomendaciones del fabricante y por lo menos una vez cada quince días.

Se deben tener interruptores eléctricos adicionales, localizados cerca de las salidas de emergencia, para lograr un rápido apagado de los sistemas en caso de una falla o contingencia. Las luces de emergencia deben funcionar en caso de fallas en la potencia eléctrica del proveedor del servicio público.

El cableado de la red lógica y eléctrica debe estar instalado y mantenido por ingenieros calificados con el fin de garantizar su integridad, operación y cumplimiento de normatividad de instalación.

Se deben realizar mantenimientos sobre los equipos de acuerdo a las recomendaciones del fabricante y realizarse únicamente por soporte técnico o personal autorizado. Si se tiene que enviar fuera de las instalaciones de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, se debe asegurar la información y verificar la vigencia y alcance de las pólizas de seguro.

9.1.6 Áreas de acceso público carga y descarga

Los puntos de acceso, tales como la entrega y las zonas de carga y otros puntos en los que las personas no autorizadas puedan entrar, se deberán controlar y, si es posible, deberán estar aisladas del procesamiento de la información en las instalaciones.

9.2 Seguridad de los Equipos

9.2.1 Emplazamiento y Protección del equipo

Los equipos de cómputo deben estar situados en el lugar designado para ello y en caso tal que se necesite mover de lugar algún dispositivo por cambio de puesto de trabajo, por

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 33 de 54

mantenimiento o dada de baja del dispositivo debe llenarse el formulario diseñado para tal fin. Los equipos deben ser protegidos para reducir los riesgos de acceso no autorizado o daño.

9.2.2 Instalaciones de suministro

El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos.

9.2.3 Seguridad del cableado

El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la interceptación, interferencia o daños.

9.2.4 Mantenimiento de los equipos

Los equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad. Por lo que se debe ejecutar mantenimientos preventivos de hardware y de software cada 3 meses. La Entidad debe contar con un cronograma de estos mantenimientos y una bitácora de registro de cumplimiento.

9.2.5 Salida de los activos fuera de las dependencias de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA

Los equipos, la información o el software no se retirarán del área física a la que pertenecen sin la previa autorización del Comité de Seguridad de la Información – CSI.

9.2.6 Seguridad de los equipos y de los activos fuera de las instalaciones

Considerando el riesgo que implica el retiro de los activos de información de las instalaciones físicas de la Entidad, los responsables de cada activo deberán tomar todas las medidas de seguridad física y lógica necesarias para salvaguardar a los activos computacionales y de la información cuando estos se encuentren fuera de las instalaciones de la Entidad.

9.2.7 Reutilización o eliminación segura de dispositivos de almacenamiento

Todas las unidades de almacenamiento que posean los sistemas computacionales que sean dados de baja o reasignados a otra dependencia de la Entidad deberán pasar antes por un proceso de eliminación segura (Wipe) con el fin de garantizar que la información sensible contenida en ellos y el software licenciado, sean eliminados de forma segura.

B9.2.8 Equipo informático de usuario desatendido

Los usuarios deberán asegurarse de que los sistemas computacionales que no sean monitoreados de forma permanente cuenten con los controles de seguridad apropiados para evitar que sean comprometidos.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 34 de 54

9.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido, el usuario deberá cerrar la sesión o deberá bloquearse la pantalla de forma automática a través del protector de pantalla con contraseña.

Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios bajo llave o con cualquier otro control que evite el acceso no autorizado, especialmente en horas no laborales de trabajo.

Información confidencial y crítica para la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe ser asegurada preferiblemente en armarios resistentes a impacto, fuego e inundación.

Los computadores personales no se deben dejarse con la sesión activa, se recomienda el uso de llaves físicas, contraseñas, y otro tipo de controles cuando no estén en uso.

Puntos de envío y recepción del correo, máquinas de fax, deben ser protegidos de acceso no autorizado.

Las fotocopiadoras deben estar protegidas de uso no autorizado.

10 SEGURIDAD EN LA OPERACIONES

10.1 Responsabilidades y Procedimientos de operación

Objetivo: Asegurar operaciones correctas y seguras de las instalaciones de procesamiento de información.

El proceso de Gestión Administrativa y tecnológica de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, es el encargado de la operación y administración de la plataforma tecnológica (Voz y Datos) que apoya los procesos de negocio, asignará funciones específicas a sus funcionarios y/o contratistas, quienes actuarán como responsables de garantizar la adecuada operación y administración de dicha plataforma, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de dichas actividades.

Los responsables de la Seguridad de la Información deben apoyar en la definición de soluciones para dar cumplimiento a los niveles de seguridad establecidos por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 35 de 54

10.1.1 Documentación de Procedimientos de operación

Los procedimientos de operación deberán ser documentados y puestos a disposición de los usuarios que los necesitan.

El proceso de Gestión Administrativa y tecnológica debe proveer a sus funcionarios de manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información (comunicaciones y servicios como correo, intranet, WEB) así como todos los componentes de la plataforma tecnológica de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

Se debe garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

10.1.2 Gestión de cambios

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA a través del área responsable establecerá, coordinará y controlará los cambios realizados en los activos de información tecnológicos y los recursos informáticos, asegurando que los cambios efectuados sobre la plataforma tecnológica, tanto el software operativo como los sistemas de información, serán debidamente autorizados por las áreas correspondientes.

El proceso de Gestión Administrativa y tecnológica debe garantizar que todo cambio realizado a un componente de la plataforma tecnológica, el cual conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes.

Se debe garantizar que todo cambio realizado sobre la plataforma tecnológica de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, quedará formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.

Los Administradores de los activos de información tecnológicos y recursos informáticos deben garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios, siguiendo el procedimiento vigente para dicha acción.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 36 de 54

10.1.3 Gestión de capacidades

El uso de los recursos será supervisado, se realizarán los ajustes pertinentes, y las proyecciones hechas de las futuras necesidades de capacidad, para asegurar el rendimiento requerido por la plataforma tecnología y administrativa.

10.1.4 Separación de entornos de desarrollo, prueba y producción

El desarrollo, las pruebas y producción deberán estar separados para reducir los riesgos de acceso no autorizado, fuga y exposición de información sensible o cambios en el entorno operativo. Se debe garantizar los recursos necesarios que permitan la separación de ambientes de desarrollo, pruebas y producción, así como de la independencia de los funcionarios que ejecutan dichas labores.

10.2 Protección contra código malicioso

Objetivo: asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra el malware.

10.2.1 Controles contra el código malicioso

Se aplicarán controles de detección, prevención y recuperación para protegerse contra el código malicioso, en combinación con el conocimiento del usuario correspondiente.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA proveerá los recursos necesarios que garanticen la protección de la información y los recursos de procesamiento de la misma adoptando controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por la contaminación y/o el contagio de software malicioso.

El proceso de Gestión Administrativa y tecnológica debe garantizar que los activos de información, así como, los recursos tecnológicos son actualizados periódicamente, evitando que código malicioso exploten vulnerabilidades de la plataforma tecnológica de la Entidad.

El proceso de Gestión Administrativa y tecnológica debe garantizar que:

- El software antimalware usado para contrarrestar los efectos del software malicioso cuenta con las licencias de uso aprobadas, garantizando su autenticidad y su periódica actualización.
- La información almacenada en los activos de información tecnológicos que es transportada por la red de datos, es escaneada con una periodicidad establecida para garantizar así la seguridad de la misma.
- Los usuarios de los activos de información tecnológicos no deben poder modificar la configuración establecida para el software antimalware.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 37 de 54

Los usuarios de los activos de información tecnológicos y recursos informáticos deben hacer uso exclusivo de hardware y software autorizado por los funcionarios del proceso de Gestión Administrativa y tecnológica.

Los usuarios de activos de información tecnológicos y recursos informáticos deben realizar la revisión de los de archivos adjuntos de los correos electrónicos antes de ser ejecutados, visualizados o abiertos de igual forma debe realizarse con los archivos de cualquier tipo descargados de cualquier fuente incluso de fuentes conocidas con el fin de reducir la posibilidad de infección, instalación y/o ejecución de malware en los sistemas computacionales de la Entidad.

Los usuarios de activos de información tecnológicos deben comunicarse con el proceso de Gestión Administrativa y tecnológica al detectar la presencia de cualquier producto de malware en sus sistemas, que no haya podido ser eliminado por el sistema antimalware local de forma automática; esto con el fin de recibir la asistencia o el soporte necesario para actuar frente a la amenaza digital

10.3 Copias de Seguridad

Objetivo: Garantizar la disponibilidad de los activos de información digitales de la Entidad.

10.3.1 Copias de seguridad de la información

Las copias de seguridad de la información, software y sistemas imágenes se tomarán y se prueban regularmente de acuerdo con una política de copia de seguridad acordada.

Los funcionarios responsables de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de la misma. Las áreas encargadas de la información en conjunto con el proceso de Gestión Administrativa y tecnológica deberán definir la estrategia a seguir para el respaldo y almacenamiento de la información.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben definir en compañía del proceso de Gestión Administrativa y tecnológica las estrategias para la correcta y adecuada generación, retención, y rotación de las copias de respaldo de la información.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben velar por el cumplimiento de los procedimientos de respaldo de la información.

El proceso de Gestión Administrativa y tecnológica debe establecer lineamientos para la generación y almacenamiento de las copias de respaldo.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 38 de 54

El proceso de Gestión Administrativa y tecnológica debe generar procedimientos para la correcta y segura generación, así como el adecuado tratamiento de las copias de respaldo.

La información que es salvaguardada por el proceso de Gestión Administrativa y tecnológica de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, deberá ser almacenada y respaldada interna y externamente a la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, de acuerdo con las normas establecidas de tal forma que se garantice su disponibilidad en cualquier momento. Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo que se realizan.

El proceso de Gestión Administrativa y tecnológica, debe contar con procedimientos para realizar pruebas a las copias de respaldo para garantizar su integridad y usabilidad en caso de ser requerido.

Los Administradores de los activos de información tecnológicos y recursos informáticos deben almacenar y respaldar las copias de seguridad según el procedimiento vigente de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, de tal forma que se garantice su confidencialidad, integridad y disponibilidad.

Los Administradores de los activos de información tecnológicos y recursos informáticos deben ejecutar los procedimientos provistos por el proceso de Gestión Administrativa y tecnológica con los medios autorizados para realizar pruebas a las copias de respaldo.

Los Administradores de los activos de información tecnológicos y recursos informáticos deben realizar pruebas periódicas de recuperación de la información respaldada y documentar sus resultados.

Se deben realizar todas las copias de respaldo de las bases de datos que contienen los sistemas de información institucionales y demás servicios, todos los días, esta tarea debe realizarse de forma automática y además cada sistema de información debe guardar los datos en tiempo real de digitación de los mismos por el usuario.

Los funcionarios y/o contratistas de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, son responsables de realizar los backups de la información institucional que cada uno maneja en sus equipos de escritorio, ya que dicha información una vez finalice el vínculo laboral con la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe ser entregada como proceso para finalizar dicha vinculación.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 39 de 54

10.4 Registro de actividad y supervisión

Objetivo: Registrar eventos y generar evidencia.

10.4.1 Registro y gestión de eventos de actividad

Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

10.4.2 Protección de los registros de información

Los registros de información se protegerán contra la manipulación y el acceso no autorizado.

10.4.3 Registros de actividad del administrador y operador del sistema

Las actividades del administrador del sistema y de la red serán registradas. Estos registros serán protegidos y regularmente revisados.

10.4.4 Sincronización de relojes

Los relojes de todos los sistemas de informática relevantes serán sincronizados a una fuente de tiempo de referencia única.

10.5 Control de software en explotación

Objetivo: Garantizar la integridad de los sistemas operativos y aplicaciones.

10.5.1 Instalación del software en sistemas en producción

Se deben implementar procedimientos para controlar la instalación de software en los sistemas operativos.

10.6 Gestión de vulnerabilidades técnicas

Objetivo: Evitar la explotación de vulnerabilidades técnicas.

10.6.1 Gestión de las vulnerabilidades técnicas

La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan se obtendrá en el momento oportuno a través de una evaluación de vulnerabilidades/ test de penetración que debe realizarse al menos una (1) vez al año por un evaluador externo. La exposición de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA a tales vulnerabilidades será evaluada y se tomarán las medidas pertinentes para hacer frente a los riesgos identificados.

10.6.2 Restricciones en la instalación de software

Las normas que regirán la instalación de software por los usuarios serán establecidas e implementadas. Los funcionarios son responsables por la instalación y utilización de

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 40 de 54

software no autorizado en sus estaciones de trabajo y en las plataformas tecnológicas que soportan los sistemas de información de la Institución.

10.7 Consideraciones de las auditorías de los sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

10.7.1 Controles de auditoría de sistemas de información

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, apoyada en la Oficina de Control Interno a través del Procedimiento de Auditoría Interna verificará el cumplimiento de los requisitos las normas ISO aplicables, la normatividad legal vigente, y los requisitos propios de la Entidad y los requisitos internos. Estas auditorías deberán tener como objetivo buscar la eficacia y eficiencia de los sistemas de información implementados en la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

Los requisitos de auditoría y las actividades relacionadas con la verificación de los sistemas operativos deberán ser cuidadosamente planificados y acordados para reducir al mínimo las interrupciones de los procesos.

11. SEGURIDAD DE LAS COMUNICACIONES

11.1 Gestión de la seguridad en las redes

Objetivo: Garantizar la protección de la información que es transmitida y transportada a través de la plataforma de red de la Entidad.

11.1.1 Controles de red

Las redes deberán ser administradas y controladas para proteger la información en los sistemas y aplicaciones.

11.1.2 Mecanismos de Seguridad asociados a servicios en red

Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red.

11.1.3 Segregación de redes

La plataforma tecnológica de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El proceso de Gestión Administrativa y tecnológica es el área encargada de establecer el perímetro de seguridad

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 41 de 54

necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe establecer mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados

11.2 Intercambio de información con partes externas

Objetivo: Mantener la seguridad de la información que se transfiere dentro de la Entidad y con cualquier GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA externa.

11.2.1 Políticas y procedimientos de intercambio de información

Los procedimientos formales de transferencia, procedimientos y controles deberán estar en posición de proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

11.2.2 Acuerdos sobre la transferencia de información

Dichos acuerdos deberán dirigirse a la transferencia segura de información comercial entre la Entidad y las partes externas.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA en su intención de proteger la información de la institución, indistintamente del lugar o forma en que está se encuentre almacenada, proveerá los recursos necesarios para garantizar la protección de la misma al momento de ser transferida, comunicada a un tercero o al salir de sus instalaciones según necesidad de la actividad o proceso particular.

El intercambio electrónico de información utilizando el canal de internet institucional, se debe realizar con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacional y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información.

Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de “no repudio”.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 42 de 54

La Gestión de Sistemas de Información y recursos tecnológicos, velará por la protección de la información, sin embargo, el contenido de los archivos enviados a través del canal de Internet institucional será directamente responsabilidad del funcionario y/o contratista.

Los responsables del intercambio de información con terceros deben definir en compañía de la Gestión de Sistemas de Información y recursos tecnológicos las estrategias para la correcta gestión e intercambio seguro de la misma.

Los responsables del intercambio de información con terceros deben diseñar, establecer y aplicar acuerdos en los cuales se definan las responsabilidades en el intercambio de información de las partes que interactúen en el mismo.

La Gestión de Sistemas de Información y recursos tecnológicos debe proveer los recursos necesarios con los cuales sea posible garantizar el correcto, adecuado y seguro intercambio de información desde estaciones de trabajo y equipos portátiles, así, como desde los dispositivos externos o móviles. Así mismo, debe garantizar que las transacciones de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA realizadas de manera electrónica o haciendo uso de las redes de comunicaciones y las estaciones de trabajo de la misma, cuentan con los controles suficientes para evitar transmisiones incompletas, enrutamiento no apropiado o erróneo, repeticiones de las mismas no autorizadas, pérdida de confidencialidad, integridad de las mismas y pérdida de disponibilidad del servicio.

Los administradores de los activos de información tecnológicos y recursos informáticos deben aplicar los controles necesarios que garantizan la disponibilidad, confidencialidad e integridad de la información transmitida electrónicamente por medio de recursos tecnológicos de propiedad o provistos por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, según necesidad o el nivel de criticidad de la misma.

Los usuarios o funcionarios tanto directos como los provistos por terceras partes que interactúen en procesos de intercambio de información al exterior de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA deben cumplir los lineamientos, recomendaciones y/o estrategias establecidas para este propósito en la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

11.2.3 Mensajería electrónica

La información involucrada en la mensajería electrónica será debidamente protegida a través de cifrado y su uso debe estar restringido al paso de información relacionada a las funciones dentro de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 43 de 54

11.2.4 Acuerdos de confidencialidad o de no divulgación

Se debe revisar, identificar y documentar regularmente los diferentes requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la Entidad para la protección de la información.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

12.1 Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad informática es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

12.1.1 Análisis y especificación de los requisitos de seguridad.

Los requisitos relacionados con la seguridad de la información serán incluidos en los requerimientos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Los responsables por la provisión de soluciones deben crear y mantener una metodología que controle el ciclo completo de adquisición, desarrollo, mantenimiento y disposición seguro de soluciones de información e infraestructura.

Los requerimientos de seguridad de la Información deben ser identificados previos al diseño o requisición de soluciones de información e infraestructura. De ser necesario el desarrollo interno, los requerimientos deben ser incluidos dentro de los sistemas y si una modificación es solicitada, debe cumplir estrictamente con los requerimientos de Seguridad de la Información que han sido previamente establecidos.

La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección ni ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como para el desarrollo de soluciones.

La información tratada por las aplicaciones aceptadas por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe preservar su confiabilidad desde su ingreso, transformación y entrega al negocio. Cada aplicación válida que use y/o transforme información del negocio debe establecer los medios que preserven su integridad y confiabilidad.

Cada solución de información o de infraestructura debe mantener durante su ciclo de vida una gestión de riesgo que informe permanentemente el nivel de exposición que representa

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 44 de 54

para la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

Cualquier cambio en el ciclo de vida de un elemento de la plataforma de operación de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe seguir los procesos de Control de Cambios y Acreditación de la instalación, para que preserve el cumplimiento de la Política.

12.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas

La información involucrada en los servicios de aplicaciones que pasan a través de redes públicas, serán protegidos de la actividad fraudulenta, el conflicto contractual y la divulgación y modificación no autorizada.

12.1.3 Protección de las transacciones por redes telemáticas

La información involucrada en las transacciones de servicios de aplicación deberá ser protegida para prevenir la transmisión incompleta, mal enrutamiento, alteración de mensaje no autorizado, la divulgación no autorizada, la duplicación de mensajes no autorizados o la reproducción.

12.2 Seguridad en los procesos de desarrollo y soporte

Objetivo: Garantizar que la seguridad informática diseñada e implementada de cumpla durante el ciclo de vida de desarrollo de sistemas de información.

12.2.1 Política de desarrollo seguro de software

Se establecerán y aplicarán reglas para el desarrollo de software de la Entidad para que se incluyan las mejores prácticas de seguridad en todas las etapas del ciclo del desarrollo de software.

12.2.2 Procedimientos de Control de cambios en los sistemas

Los cambios en los sistemas dentro del ciclo de desarrollo deberán cumplir los procedimientos formales de control de cambios.

12.2.3 Revisión técnica de las aplicaciones después de efectuar cambios en los sistemas operativos

Cuando se cambian las plataformas de operación, las aplicaciones críticas deberán ser revisadas y probadas para asegurar que no hay impacto negativo en las operaciones de la Entidad o de la seguridad.

12.2.4 Restricciones a los cambios en los paquetes de software

Las modificaciones a paquetes de software serán disuadidas, limitadas a cambios necesarios y todos los cambios estrictamente serán controlados.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 45 de 54

12.2.5 Uso de principios de ingeniería en protección de sistemas

Se aplicarán los principios de ingeniería de sistemas seguros, se documentará, y aplicará en la implementación de cualquier sistema de información.

12.2.6 Entorno de desarrollo seguro

El proceso de Gestión Administrativa y tecnológica debe definir y establecer formalmente la documentación requerida en las diferentes etapas de ciclo de vida de los sistemas.

12.2.7 Desarrollo tercerizado

El proceso de Gestión Administrativa y tecnológica debe contar con un grupo de personas el cual debe autorizar la creación, adaptación o adquisición de software.

Los contratos de consultoría, y en general todo tipo de contratos de servicios deben contener provisiones a este respecto. De igual manera, dada la proliferación del “outsourcing”, es especialmente importante clarificar los derechos generados por proveedores en desarrollo de este tipo de contratos.

12.2.8 Pruebas de funcionalidad durante el desarrollo de los Sistemas

Las pruebas de la funcionalidad se deben llevar a cabo durante el desarrollo del sistema.

12.2.9 Pruebas de aceptación del sistema

Se debe cumplir con los formatos y el procedimiento del sistema de calidad para la realización y documentación de las pruebas de funcionalidad y seguridad.

12.3 Los datos de prueba

Objetivo: Garantizar la protección de los datos utilizados para la prueba.

12.3.1 Protección de los datos de prueba

Los datos de prueba deben seleccionarse cuidadosamente, en caso de tener que seleccionar datos reales estos deben ser protegidos y controlados.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 46 de 54

13. RELACIONES CON LOS PROVEEDORES

13.1 Seguridad de la información en relación con los proveedores

Objetivo: Garantizar la protección de los activos de la Entidad que sea accesible por los proveedores.

13.1.1 Política de seguridad de la información para las relaciones con proveedores

Se acordará con el proveedor y se documentaran los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la Entidad.

De igual forma se debe incluir un acuerdo formal de Niveles de Servicios en Seguridad de la Información, en el que se detallen los compromisos en el cuidado de los recursos de Información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA y las sanciones en caso de incumplimiento. El cumplimiento de los Niveles de Servicios en Seguridad de la Información de terceros debe ser verificado y controlado permanentemente por quienes ejerzan las funciones de interventoría de los contratos suscritos por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA. Cuando la interventoría sea contratada, se debe incluir esta obligación dentro de los Contratos. En el caso en que la interventoría sea realizada por funcionarios de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, se entiende que el cumplimiento de la Política está incorporado dentro de sus obligaciones como funcionario y como interventor.

13.1.2 Tratamiento del riesgo dentro de acuerdos con proveedores

Todos los requisitos de seguridad de la información pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

13.1.3 Cadena de suministro en tecnologías de la información y comunicaciones

Incluir los requisitos para los acuerdos con proveedores para abordar los riesgos de la seguridad de la información asociada con los servicios de las tecnologías de información y comunicación y de la cadena de suministro de productos.

13.2 Gestión de la prestación de servicios por proveedores

Objetivo: Mantener un nivel convenido de seguridad de la información y la prestación de servicios en los acuerdos con los proveedores.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 47 de 54

13.2.1 Seguimiento y revisión de los servicios de proveedores

Cada servicio con proveedor deberá tener con un supervisor encargado de revisar y auditar la prestación de servicios de proveedores.

13.2.2 Gestión de cambios en los servicios prestados por proveedores

Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y re-evaluación de los riesgos.

14. GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN

14.1 Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Garantizar un enfoque coherente y eficaz para la gestión de incidentes en la seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la Información.

El responsable de la Información debe definir los eventos considerados como críticos junto con sus respectivas alertas y registros de seguridad de la información, los cuales deberán ser generados. Éstos deben ser activados, vigilados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera inmediata al equipo de respuesta a Incidentes. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las evidencias.

Los incidentes de seguridad, resultantes del incumplimiento de la Política y Normas de seguridad de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA serán direccionados por el Procedimiento de manejo de incidentes establecido por el área del proceso de Gestión Administrativa y tecnológica, con el objetivo de realizar la respectiva investigación y entregar los resultados a los respectivos responsables dentro de la Entidad, encargados de tomar las acciones correctivas y preventivas del caso.

Los funcionarios deberán estar informados del proceso disciplinario que se llevará a cabo en caso de incumplimiento de la Política de Seguridad de la Información o alguno de los elementos que la soportan. En cualquier caso, se hará un seguimiento de acuerdo con los procedimientos establecidos para el manejo de incidentes de seguridad.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 48 de 54

14.1.1 Responsabilidades y procedimientos

La responsabilidad y el procedimiento de manejo para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información está en cabeza del proceso de Gestión Administrativa y tecnológica.

14.1.2 Informar sobre los eventos de seguridad de información

Los eventos de seguridad de información se comunicarán a través de canales de gestión adecuadas tan pronto como sea posible.

14.1.3 Notificación de puntos débiles de la seguridad

Los funcionarios y contratistas que utilizan los sistemas y servicios de información deben observar y reportar cualquier debilidad de seguridad de información observada o sospechada en los sistemas o servicios.

14.1.4 Valoración de eventos de seguridad de la información y toma de decisiones

El proceso de Gestión Administrativa y tecnológica es el encargado de valorar los eventos de seguridad de información y decidir si han de ser clasificados como incidentes de seguridad de la información.

14.1.5 Respuesta a incidentes de seguridad de la información

Los incidentes de seguridad de información deberán recibir una respuesta de conformidad con los procedimientos documentados.

14.1.6 Aprendizaje de los incidentes de seguridad de la información

Los conocimientos adquiridos a partir del análisis y la resolución de incidentes de seguridad de información se deben utilizar para reducir la probabilidad o el impacto de los incidentes en el futuro.

14.1.7 Recopilación de evidencias

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia en un caso de análisis forense.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 49 de 54

15. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

15.1 Continuidad de la seguridad de la Información

Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.

Los procesos críticos establecidos por la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, deben garantizar que sus activos de información estén disponibles para su tratamiento autorizado cuando la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA lo requiera en la ejecución de sus tareas regulares. Se debe definir e implementar un proceso para reducir la interrupción causada por desastres naturales, accidentes y fallos de seguridad por medio de la combinación de controles preventivos y de recuperación.

Para los procesos críticos del negocio, la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad del negocio aún en caso de desastre en las instalaciones de los lugares de operación.

Cada lugar debe incluir los controles establecidos para éste tipo de áreas según su clasificación, para que no se vea disminuido los aspectos de seguridad en caso de desastre.

Por razones de la continuidad en la operación normal del negocio se debe contar con circuitos alternos y equipos que suministren energía en caso de una falla. Es necesario contar con servicios de mantenimiento periódico a estos equipos y realizar pruebas programadas a los mismos para estar siempre en posibilidad de prestar servicio sin interrupciones a los usuarios.

Se debe seguir una estrategia de recuperación alineada con los objetivos de negocio, formalmente documentada y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos del negocio, ante el evento de una contingencia.

Cada responsable de los procesos de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA con el acompañamiento del proceso de Gestión Administrativa y tecnológica, debe diseñar, implementar, probar y mantener su Plan de Continuidad.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 50 de 54

El plan de continuidad debe considerar los siguientes aspectos:

- Procedimientos de contingencia. Los cuales describen las acciones a tomar cuando ocurre un incidente que interrumpe las operaciones del negocio, proporcionando mecanismos alternos y temporales para continuar con el procesamiento.
- Procedimientos de recuperación. Los cuales describen las acciones a seguir para trasladar las actividades del negocio a un centro alternativo de recuperación.
- Procedimientos de retorno. Los cuales describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.

Planificación de las pruebas. Las cuales describen la periodicidad en que el plan de continuidad debe ser probado.

- Actualización periódica. El plan debe actualizarse cuando cambios realizados en el ambiente operativo impacten su funcionalidad.
- Consideraciones de seguridad. Es importante que el plan sea diseñado para mantener los controles de seguridad establecidos por la Entidad, aun cuando se opere en modalidad de contingencia. Es responsabilidad de la Coordinación de Seguridad de la Información asegurar que estas consideraciones sean efectivamente contempladas en el plan.
- Cuando se realicen pruebas, simulacros o se tengan contingencias reales, los resultados y sugerencias deben ser entregadas a los responsables de la información quienes deben actualizar sus planes y mantenerlos al día conforme los riesgos de disponibilidad lo dictaminen.
- El proceso de copia y respaldo de la información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe contar con una Política que debe cumplir con los requerimientos del negocio, los de seguridad de la información y los legales. Este proceso junto con sus procedimientos es la entrada para la ejecución de los planes de Continuidad de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, en caso de presentarse un evento que amerite la activación del Plan.

15.1.1 Planificación de la continuidad de la seguridad de la información y Análisis de riesgos

Análisis de riesgos enfocado específicamente a valorar el impacto de incidentes que comprometen la continuidad del negocio teniendo en cuenta que este impacto será mayor cuanto más dure el incidente. Los pasos a seguir para realizarlo son los habituales de un análisis de riesgos:

- Se identifican los procesos críticos de negocio.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 51 de 54

- Se identifican los eventos que pueden provocar interrupciones en los procesos de negocio de la Entidad, p. ej. fallos de los equipos, errores humanos, robos, incendios, desastres naturales y actos terroristas.
- Se evalúan los riesgos para determinar la probabilidad y los efectos de dichas interrupciones en cuanto a tiempo, escala de daños y período de recuperación.
- Se Identifican los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información en el ámbito del sistema de gestión de la seguridad de información, y establece acciones de control y responsables de contribuir en la mitigación de los riesgos.

15.1.2 Implantación de la continuidad de la seguridad de la información

Establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

15.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Verificar la información de continuidad de los controles de seguridad establecidos y aplicados a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas.

15.2 Redundancias

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

15.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

Las instalaciones para el procesamiento de información deben contar con la suficiente redundancia para satisfacer los requisitos de disponibilidad.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 52 de 54

16. CUMPLIMIENTO

16.1 Cumplimiento de los requisitos legales y contractuales

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisitos de seguridad.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas, resueltas y reportadas de manera inmediata a través de los canales señalados para el efecto.

Se entenderán incluidas a la Política las regulaciones nacionales e internacionales que de tiempo en tiempo se expidieren y que se relacionen con la misma.

Cuando de la aplicación de tales normas se presentare un conflicto, se entenderá que aplica la más restrictiva, es decir, aquella que exija el mayor grado de seguridad.

Así mismo y con el fin de mantener un nivel de seguridad adecuado con el negocio de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, esta Política se debe apoyar en las mejores prácticas de seguridad de la información y aquellas que el mercado y la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA reconozcan como tal.

La Política junto con el Proceso de Gestión de Información y Tecnología del Sistema de Gestión de Calidad de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA debe ser auditada anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.

La información de auditoría generada por el uso de los controles de seguridad de los Recursos de Tecnología, debe ser evaluada por el responsable para:

- Detectar Violaciones a la Política.
- Reportar incidentes de seguridad.
- Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.

Periódicamente se debe evaluar el cumplimiento de los requerimientos de seguridad por parte de los Usuarios. El incumplimiento de los requerimientos de seguridad, se debe registrar como un incidente a la Política de Seguridad de la información que debe ser resuelto de acuerdo con los procedimientos de manejo de incidentes de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 53 de 54

Deben establecerse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de material que puede estar sujeto a derechos de propiedad intelectual tales como derechos de autor y derechos de diseño.

16.1.1 Identificación de la legislación aplicable y los requisitos contractuales

Todos los requisitos pertinentes, legislativos estatutarios, reglamentarios y contractuales, y el planteamiento de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA para cumplir con estos requisitos deberán estar explícitamente identificados, documentados y protegidos al día para cada sistema de información y la Entidad.

16.1.2 Derechos de propiedad intelectual

Se aplicarán procedimientos apropiados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales, relacionados con los derechos de propiedad intelectual y uso de productos de software propietario.

Se debe establecer en los contratos de trabajo de funcionarios y en los contratos de desarrollo realizados por proveedores y contratistas, cláusulas respecto a la propiedad intelectual de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA, al material y productos generados en el desarrollo del negocio.

16.1.3 Protección de los registros

Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requisitos de legalidad, reglamentarias, contractuales y comerciales.

16.1.4 Protección de datos y privacidad de la información personal

Se garantizará la privacidad y la protección de la información de identificación personal a lo dispuesto en la legislación y la reglamentación pertinente en su caso.

16.1.5 Regulación de los controles criptográficos

Los controles criptográficos serán utilizados en cumplimiento a todos los acuerdos pertinentes, la legislación y los reglamentos.

16.2 Revisiones de la seguridad de la información

Objetivo: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos de la Entidad.

16.2.1 Revisión independiente de la seguridad de la información

El enfoque de la Entidad para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	Fecha de Aprobación:	Código:
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01	Página 54 de 54

16.2.2 Cumplimiento de las políticas y normas de seguridad

El proceso de Gestión Administrativa y tecnológica deberá comprobar periódicamente el cumplimiento de los procedimientos de procesamiento de la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.

16.2.3 Comprobación del cumplimiento

Los sistemas de información deben ser revisados regularmente para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas, resueltas e informadas al comité de Seguridad de la Información y a las áreas responsables por su tratamiento de manera inmediata.