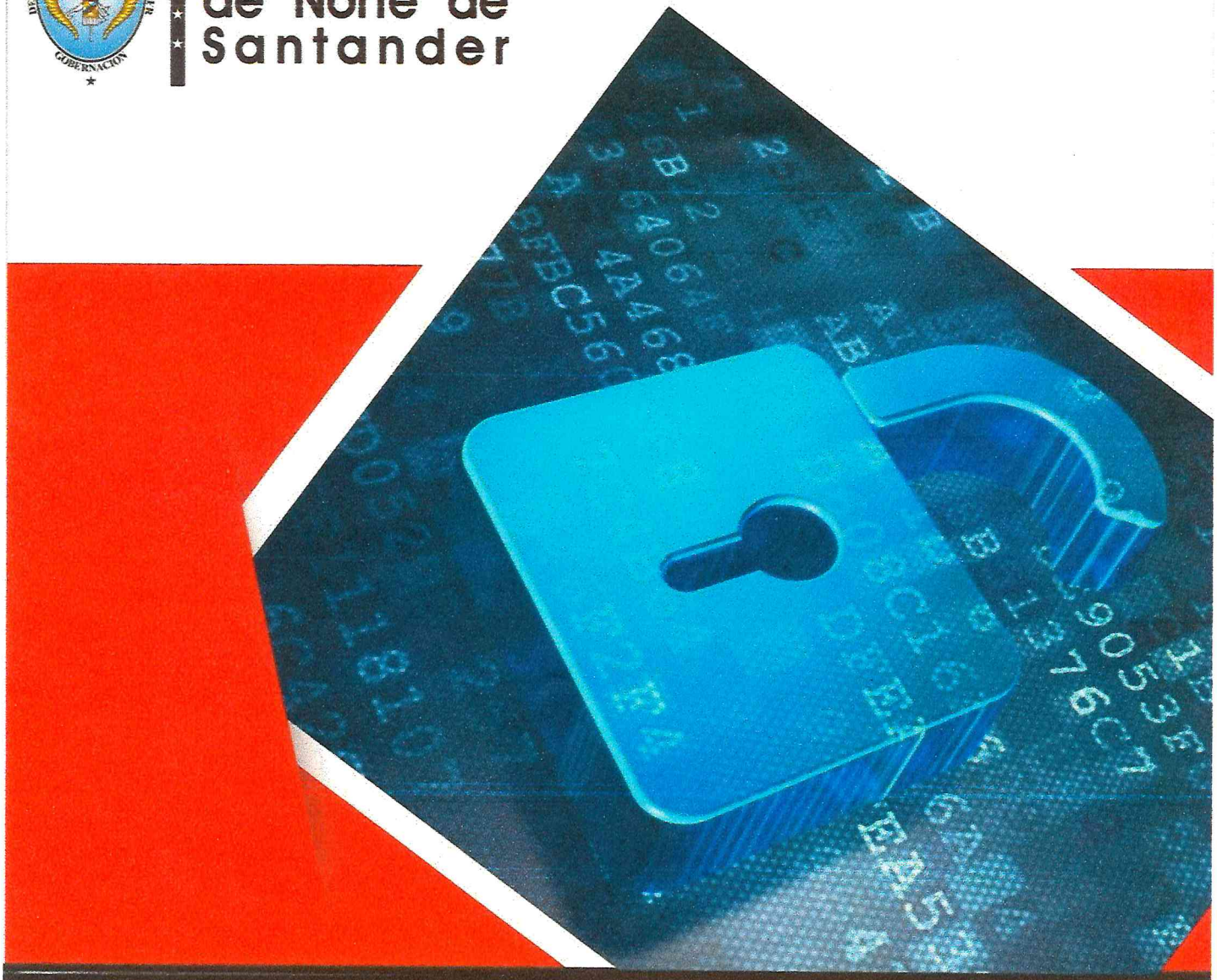
Gobernación de Norte de Santander



POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

SECRETARIA DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONNES

UN NORTE PRODUCTIVO PARA TODOS

Plan de Desarrollo 2016 -2019

Contenido

CREDITOS

Versión 1.0

Marina Lozano Ropero
Secretaria de las Tecnologías de las Información y Comunicaciones

Christian Alfonso Saravia Uribe
Ingeniero de Sistemas - Secretaria de las Tecnologías de las Información y Comunicaciones

Diseño de Portada
http://www.freepik.com">Designed by new7ducks
https://www.canstockphoto.es/azul-abierto-candado-plano-de-fondo-15027105.html

ALCANCE

La Gobernación de Norte de Santander en su interés de avanzar a la par con la tecnología y a medida que se van adquiriendo sistemas de información, equipos tecnológicos entre otros, ve la necesidad de dar la importancia requerida a la información y/o datos que son generados en cada una de las Secretarias, Oficinas y Altas Consejerías.

Por lo anterior la presente política de seguridad brinda unos lineamientos basados en un marco legal vigente, a todos los funcionarios de la Gobernación de Norte de Santander y usuarios externos, con el único fin de mantener con cierto nivel de privacidad, entereza y total disposición de la información y/o datos de la entidad.

OBJETIVO

Planear, organizar, dirigir, mantener, controlar y garantizar la integridad física de los recursos informáticos, y brindar una herramienta que sirva para dotar de información necesaria al Gobernador, Secretarias, Oficinas, Altas Consejerías, Funcionarios de Planta, Contratistas y Usuarios Externos, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software, así como la información y/o datos que son procesados y almacenados en cada una de las dependencias. De esta manera resguardar los activos de la Gobernación de Norte de Santander.

Objetivos Específicos

- Brindar a los usuarios internos y/o externos de la Gobernación de Norte de Santander un entorno de confianza digital en el uso y aprovechamiento de las TIC para garantizar la gobernanza, derechos, satisfacción de necesidades y la prestación de trámites y servicios, seguros y con calidad.
- Servir como requisito habilitador en la relación estado - sociedad donde el primero sea consolidado como generador de información y prestador de servicios; y el segundo como ciudadanos competitivos, productivos e innovadores.

MARCO LEGAL

- Ley 527 de 1999. Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio el cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Ley 1712 de 2014. Ley de transparencia y del derecho al acceso de la información pública nacional.
- Decreto 1078 del 26 de mayo de 2015. Por medio el cual se expide el Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 del 14 de junio de 2018. Por medio el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

VIGENCIA

Las amenazas a las que está expuesta la infraestructura tecnológica se encuentran en continuo proceso de expansión, lo que, unido al progresivo aumento de los sistemas de información y usuarios de estos, hace que todos los sistemas y aplicaciones estén expuestos a riesgos cada vez mayores, que sin una adecuada gestión de los mismos, pueden ocasionar que su vulnerabilidad se incremente y consiguientemente los equipos o sistemas sean afectados.

Todo servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) son responsables del cumplimiento de los estándares, directrices y procedimientos de control de acceso, así como también notificar a la Secretaría TIC, cuando por algún motivo no pueda cumplir con las Políticas de Seguridad indicando el motivo por el cual no le es posible ceñirse a la normativa de seguridad.

Cabe destacar que este nivel de responsabilidad va a ser conocido por las diferentes Secretarías, Oficinas y Altas Consejerías de la Gobernación, quienes serán las garantes de que esta información sea conocida por cada integrante de dichas secretarías o áreas. La documentación presentada como Política de Seguridad entrará en vigencia desde el momento en que sean aprobadas por el Gobernador. Esta normativa deberá ser revisada y actualizada por lo menos una vez al año o conforme a las exigencias de la Gobernación de Norte de Santander o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La dirección de la **GOBERNACION DE NORTE DE SANTANDER**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la **GOBERNACION DE NORTE DE SANTANDER**, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la **GOBERNACION DE NORTE DE SANTANDER** según como se defina en el alcance, sus servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratistas), terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes 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 ciudadanos, aliados estratégicos y servidores públicos.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los Servidores Públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratistas), terceros, aprendices, practicantes, proveedores de la **GOBERNACION DE NORTE DE SANTANDER.**
- Garantizar la continuidad del negocio y/o servicio frente a incidentes.

- La **GOBERNACION DE NORTE DE SANTANDER** ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación se establecen 11 principios de seguridad que soportan el SGSI de la **GOBERNACION DE NORTE DE SANTANDER**:

- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratistas), terceros, aprendices, practicantes, proveedores.

- La **GOBERNACION DE NORTE DE SANTANDER protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o contratistas), o como resultado de un servicio interno en outsourcing.

- La **GOBERNACION DE NORTE DE SANTANDER protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La **GOBERNACION DE NORTE DE SANTANDER protegerá su información** de las amenazas originadas por parte del personal.

- La **GOBERNACION DE NORTE DE SANTANDER protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

- La **GOBERNACION DE NORTE DE SANTANDER controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La **GOBERNACION DE NORTE DE SANTANDER implementará control de acceso** a la información, sistemas y recursos de red.

- La **GOBERNACION DE NORTE DE SANTANDER** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La **GOBERNACION DE NORTE DE SANTANDER** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- La **GOBERNACION DE NORTE DE SANTANDER garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- La **GOBERNACION DE NORTE DE SANTANDER** garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

NOTIFICACIONES DE VIOLACION DE SEGURIDAD

Es de carácter obligatorio para todo servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista), la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse por escrito vía correo electrónico a la Secretaría TIC, que está en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente. Es responsabilidad de todo servidor público que maneje datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, puesto que estas descansan en el establecimiento de responsabilidades donde se incurra en alguna violación en materia de seguridad acarreando sanciones a quien las haya causado, puesto que esto ocasionaría perjuicios económicos a la Gobernación de Norte de Santander de diversas consideraciones.

Es por ello que las personas relacionadas de cualquier forma con los procesos tecnológicos deben ser conscientes y asumir que la seguridad es asunto de todos y, por tanto, se debe conocer y respetar las Políticas de Seguridad. Está fundamentado como una exigencia que los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) de este ente conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación o falta. Por esta razón se entenderá que sólo una adecuada política de seguridad tecnológica apoyará la concientización para obtener la colaboración de los servidores públicos, haciéndoles conscientes de los riesgos que podemos correr y de la importancia del cumplimiento de las normas.

- Lineamientos para la adquisición de bienes informáticos

Toda adquisición de equipos tecnológicos o informáticos se efectuará bajo plena revisión o visto bueno de la Secretaría TIC. Al planear las operaciones correspondientes a la adquisición de bienes informáticos, se establecerán prioridades y en la selección deberá tomar en cuenta:

- ✓ Precio Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.
- ✓ Calidad Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.
- ✓ Experiencia, Presencia en el mercado, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.
- ✓ Desarrollo Tecnológico, Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.
- ✓

ESTANDARES

Toda adquisición se basa en los estándares, es decir la arquitectura definida por la Secretaría TIC. Esta arquitectura tiene una permanencia o vigencia mínima de dos a cuatro años.

Capacidades:

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo.

Para la adquisición de Hardware se tendrá en cuenta lo siguiente:

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de la Gobernación de Norte de Santander.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
- Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados.
- La marca de los equipos o componentes tecnológicos deberá contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local.

Tratándose de microcomputadores, a fin de mantener actualizada la arquitectura informática de la Gobernación, la Secretaría TIC emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.

- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado, corroborando que los suministros (tintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
- Los equipos adquiridos deben contar con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los servidores, equipos de comunicaciones, routers, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos al vencer su período de garantía.
- En lo que se refiere a los computadores personales, al vencer su garantía por adquisición, deberán de contar por lo menos con un programa de servicio de mantenimiento preventivo y correctivo que incluya el suministro de repuestos.
- Todo proyecto de adquisición de bienes de tecnología, debe sujetarse al análisis, aprobación y autorización de la Secretaría TIC.

SOFTWARE

En la adquisición de equipos tecnológicos o de cómputo se deberá incluir el software vigente precargado con su licencia correspondiente. Para la adquisición de software base y utilitarios, la Secretaría TIC dará a conocer periódicamente las tendencias con tecnología de punta vigente.

Licenciamiento

- Todos los productos de Software que se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.
- La Secretaría TIC promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

Para la operación del software de red en caso de manejar los datos empresariales mediante sistemas de información, se deberá tener en consideración lo siguiente:

- Toda la información de la Gobernación de Norte de Santander deberá invariablemente ser operada a través de un mismo tipo de sistema o motor de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.
- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los DVDs, Blue Ray o Discos Externos de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo (Google Drive) o en medios de almacenamiento alternos.
- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Un manual técnico que describa la estructura interna del sistema así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema y los procedimientos para su utilización.
- Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoria y Control).

- Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

Frecuencia de evaluación de las políticas.

Se evaluarán las políticas del presente documento, con una frecuencia anual por la Secretaría TIC.

POLITICAS DE SEGURIDAD FISICA

Acceso Físico

La Gobernación de Norte de Santander destinará un área que servirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y servidores. Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario, funcionario o persona no autorizada, no tenga acceso físico directo.

Entendiendo por sistema de comunicaciones: servidores, equipo activo y los medios de comunicación.

El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por la Secretaría TIC.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable de la Secretaría TIC.

Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido. El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el responsable, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del Área Administrativa de la Gobernación de Norte de Santander y al personal de seguridad del edificio.

Protección Física

El Data Center deberá:

- Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.

- Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por la Secretaría TIC.
- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- Aire acondicionado. Mantener la temperatura a 21 grados centígrados.
- Asignar un responsable para que realice un control diario temperatura y aires acondicionados y llevar un registro de estos controles.
- Respaldo de energía redundante.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Contar con algún esquema que asegure la continuidad del servicio.
- Control de humedad.
- Prevención y/o detección de incendios
- Sistemas de extinción.
- Contar por lo menos con dos extintores de incendio adecuado y cercano al Data Center (Tipo Gas: FM200 y HCFC-123, el FM 200 se recomienda es uno de los gases que daña menos la capa de ozono y uno de los que menos perjudica al ser humano, por el porcentaje de oxigeno que consume en el ambiente a extinguir).

Infraestructura

Las secretarías, oficinas y altas consejerías deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

El resguardo de los equipos de cómputo deberá quedar bajo la secretaría TIC contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- La Secretaría TIC, deberá contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones de los equipos de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

Control

- La secretaría TIC deberá llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.
- La Secretaría TIC son los responsables de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.
- La Secretaría General deberá reportar a La Secretaría TIC cuando un servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) deje de laborar o de tener una relación con la Gobernación de Norte de Santander con el fin de retirarle las Políticas de Seguridad Informática y supervisar la correcta devolución de los equipos y recursos asignados al funcionario.
- El servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista), en caso de retiro, deberá tramitar ante la Secretaría TIC el documento paz y salvo correspondiente.

Respaldos

- Las Bases de Datos de la Gobernación de Norte de Santander serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro (Cloud).
- Los demás respaldos (una copia completa) deberán ser almacenados en un lugar seguro y distante del sitio de trabajo, en bodegas con los estándares de calidad para almacenamiento de medios magnéticos.
- Para reforzar la seguridad de la información, los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista), bajo su criterio, deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio; Los respaldos serán responsabilidad absoluta de los funcionarios (Planta, Contratista).

- La Secretaría TIC no podrá remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

RECURSOS DE LOS USUARIO

Uso

- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) deberán cuidar, respetar y hacer un uso adecuado de los recursos de tecnología o cómputo y red de la Gobernación de Norte de Santander, de acuerdo con las políticas que en este documento se mencionan.
- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) deberán solicitar apoyo a la Secretaría TIC ante cualquier duda en el manejo de los recursos de tecnología o cómputo de la Gobernación de Norte de Santander.
- El correo electrónico institucional no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la Gobernación, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera). El acceso y manejo de esta herramienta tecnológica está regulada por la guía de uso y apropiación de correos institucionales adoptada mediante resolución 517 del 31 de mayo de 2017.

DERECHOS DE AUTOR

Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los usuarios deberán firmar un documento donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor.

Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la Gobernación de Norte de Santander bajo ninguna circunstancia sin la autorización escrita de la Secretaria TIC.

No está permitido instalar ningún programa en su computadora sin dicha autorización o la clara verificación de que la Gobernación de Norte de Santander posee una licencia que cubre dicha instalación.

- No está autorizada la descarga de internet de programas informáticos no autorizados por La Secretaría TIC.
- No se tolerará que un funcionario (planta, contratista) realice copias no autorizadas de software o programas de cómputo.
- No se tolerará que un servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) cargue o descargue software o programas de cómputo no autorizados de internet, incluidos entre otros la descarga de programas para utilizar sistemas de peer-to-peer (P2P – Ej. Limewire, Kazaa, Edonkey, Emule) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.
- No se tolerará un servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) realice intercambios o descargas de archivos digitales de música (MP3, MP4, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.
- Si se descubre que un servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) ha copiado software, programas informáticos o música en forma ilegal, se verá expuesto a las sanciones disciplinarias establecidas en la Ley 734 de 2002 "Por la cual se expide el código disciplinario único".
- Si se descubre que un servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) ha copiado software o programas informáticos en forma ilegal para dárselos a un tercero, se verá expuesto a las sanciones disciplinarias establecidas en la Ley 734 de 2002 "Por la cual se expide el código disciplinario único".
- Si un servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) desea utilizar programas informáticos autorizados por la Gobernación de Norte de Santander en su hogar, debe consultar con la Secretaría TIC para asegurarse de que ese uso esté permitido por la licencia del editor.
- El personal encargado de soporte de la Secretaría TIC revisará las computadoras constantemente para realizar un inventario de las instalaciones de software o programas informáticos y determinar si la Gobernación de Norte de Santander posee licencias para cada una de las copias de los programas instalados.
- Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.
- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) utilizarán el software o programas

informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas del software o programas informáticos comerciales.

- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) no descargarán ni cargarán software o programas informáticos no autorizados a través de Internet.
- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) que se enteren de cualquier uso inadecuado que se haga en la Gobernación de Norte de Santander del software o programas informáticos o la documentación vinculada a estos, deberán notificar a la Secretaria TIC.
- Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de software o programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la copia o duplicación ilegal de software o programas informáticos.
- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) que realicen, adquieran o utilicen copias no autorizadas de software o programas informáticos estarán expuestos se verá expuesto a las sanciones disciplinarias establecidas en la Ley 734 de 2002 "Por la cual se expide el código disciplinario único". Dichas sanciones pueden incluir suspensiones y despidos justificados.

POLITICAS DE SEGURIDAD LOGICA

Red

- Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de la Gobernación de Norte de Santander entre los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) y hacia afuera a través de conexiones con otras redes.
- La Secretaría TIC no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) responsable del equipo.
- No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de Las Gobernación de Norte de Santander.

- Las cuentas de ingreso a los sistemas y los recursos de tecnología o cómputo son propiedad de la Gobernación de Norte de Santander y se usarán exclusivamente para actividades relacionadas con la labor asignada.
- Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario o vigencia del contrato.
- El uso de analizadores de red es permitido única y exclusivamente por La Secretaría TIC para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las Políticas de Seguridad.
- No se permitirá el uso de analizadores para monitorear o censar redes ajenas a la Gobernación de Norte de Santander y no se deberán realizar análisis de la Red desde equipos externos al ente.
- Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

Servidores

Configuración e instalación La Secretaría TIC tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

- La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de La Secretaría TIC.
- Durante la configuración de los servidores La Secretaría TIC debe generar las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista).
- Los servidores que proporcionen servicios a través de la red e Internet deberán: Funcionar 24 horas del día los 365 días del año. Recibir mantenimiento preventivo mínimo dos veces al año; Recibir mantenimiento semestral que incluya depuración de logs. Recibir mantenimiento anual que incluya la revisión de su configuración. Ser monitoreados por la Secretaría TIC.
- La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo: Diariamente, información crítica. Semanalmente, los documentos web. Mensualmente, configuración del servidor y logs.
- Los servicios hacia Internet sólo podrán proveerse a través de los servidores autorizados por la Secretaría TIC.

Correo Electrónico Institucional

- La Secretaría TIC se encargarán de asignar las cuentas a los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) para el uso de correo electrónico en los servidores que administra.
- Para efecto de asignarle su cuenta de correo a los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista), la Secretaria General área de Talento Humano deberá realizar una solicitud para tal fin y comunicarlo a la Secretaría TIC.
- La cuenta será activada en el momento en que los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.
- La longitud mínima de las contraseñas será igual o superior a nueve caracteres, debe ser alfanumérica y debe de contener al menos un carácter especial (Ej. @, +, *).
- El uso de los correos electrónicos institucionales son de carácter obligatorio dentro de la operación de los procesos, funciones y actividades que cumple cada servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) en la entidad.

Bases de Datos

- El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.
- El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.
- Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.
- En caso de olvido de contraseña de un servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista), será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

RECURSOS DE CÓMPUTO

Seguridad del Sistema

- La Secretaría TIC es la encargada de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en los equipos, sistemas de información y red. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.
- La Secretaría TIC debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los equipos o sistemas de cómputo.
- La Secretaría TIC es la única dependencia autorizada para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

INGENIEROS DE SOPORTE

Atribuciones y/o responsabilidades

- Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.
- Deberán utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.
- Deberán realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.
- Deben actualizar la información de los recursos tecnológicos o de cómputo de la Gobernación de Norte de Santander, cada vez que adquiera e instale equipos o software.

- Deben registrar cada máquina en el inventario de recursos tecnológicos o equipos de cómputo y red de la Gobernación de Norte de Santander.
- Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Realizar la instalación o adaptación de sus sistemas de información de acuerdo con los requerimientos en materia de seguridad.
- Reportar al funcionario encargado los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de información.

RENOVACION DE EQUIPOS

- Se deberán definir los tiempos estimados de vida útil de los equipos tecnológicos o equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.
- Cuando las Secretarías, oficinas o altas consejerías requieran de un equipo tecnológico o equipo de cómputo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al Secretaría TIC a fin de que se seleccione el equipo adecuado, esta última a su vez establecerá las condiciones técnicas de los equipos acorde a las necesidades tecnológicas de cada oficina, estas condiciones deberán estar contenidos en los estudios previos a la contratación de adquisición o compra de equipos.

USO DE SERVICIOS DE RED

Secretarías, Oficinas y Altas Consejerías

- La Gobernación de Norte de Santander definirá los servicios de Internet a ofrecer a los funcionarios y se coordinará con La Secretaría TIC para su otorgamiento y configuración.
- La Gobernación de Norte de Santander puede utilizar la infraestructura de la Red para proveer servicios a los usuarios externos previa autorización de la Secretaría TIC.

- La Secretaría TIC son los responsables de la administración de contraseñas y deberán guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.
- No se asignara equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en la Gobernación de Norte de Santander

.

La Secretaría TIC realizará las siguientes actividades en los servidores de la Gobernación de Norte de Santander:

- ✓ Respaldo de información conforme a los procedimientos establecidos.
- ✓ Revisión de logs y reporte de cualquier eventualidad.
- ✓ Implementar de forma inmediata las recomendaciones de seguridad y reportar posibles faltas a las políticas de seguridad en tecnología e Informática.
- ✓ Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
- ✓ Organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.

• La Secretaría TIC es el único autorizado para asignar las cuentas a los usuarios.

• La Secretaría TIC podrá aislar cualquier servidor de red, notificando a las Secretarías, Oficinas y Altas Consejerías de la Gobernación, en las condiciones siguientes:

- ✓ Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.
- ✓ Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
- ✓ Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
- ✓ Si se detectan accesos no autorizados que comprometan la integridad de la información.
- ✓ Si se viola las políticas de uso de los servidores.
- ✓ Si se reporta un tráfico adicional que comprometa a la red de la Gobernación de Norte de Santander.

USUARIOS

Identificación de Usuarios y contraseñas

- Todos los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) con acceso a un sistema de información o a la Red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Ningún servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) recibirá un identificador de acceso a la Red, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.
- El servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.
- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) tendrán acceso autorizado únicamente a aquellos datos y recurso que precisen para el desarrollo de sus funciones o razón, objeto de contrato, conforme a los criterios establecidos por La Secretaria TIC.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Los identificadores para funcionarios (Contratista) temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- El servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud de la Secretaria TIC, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:

  - ✓ Cuando ésta sea una contraseña débil o de fácil acceso.
  - ✓ Cuando crea que ha sido violada la contraseña de alguna manera.

- El servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) deberá notificar a la Secretaria TIC en los siguientes casos:

  - ✓ Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
  - ✓ Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

- Si un usuario viola las políticas de uso de los servidores, la Secretaría TIC podrá cancelar totalmente su cuenta de acceso a los servidores, notificando a La Secretaría correspondiente.

Responsabilidades Personales

- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- Los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- Si un servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar y éste reportar al responsable de la administración de la red de la Secretaria TIC.
- El servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.
- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

- En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 3 meses.
- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.
- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.
- Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

Uso Apropiado de los Recursos

Los Recursos Tecnológicos, Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para complementar las obligaciones y propósito de la operatividad para la que fueron adquiridos, diseñados e implantados.

Prohibiciones

- El uso de estos recursos para actividades no relacionadas con el propósito de la razón, objeto o negocio de su trabajo, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Tecnológicos o Informáticos propios de Las Empresas.
- Introducir en los Sistemas de Información o la Red de la Gobernación de Norte de Santander contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, malware, virus, software espía, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Tecnológicos o Informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio,

deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

ANTIVIRUS

Antivirus de la Red

- Todos los equipos de cómputo de la Gobernación de Norte de Santander deberán tener instalada una Solución Antivirus.
- Periódicamente se hará el rastreo en los equipos tecnológicos o de cómputo de la Gobernación de Norte de Santander, y se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

RESPONSABILIDADES DE LAS SECRETARIA TIC

La Secretaría TIC será responsable de:

- Implementar la Solución Antivirus o antimalware en las computadoras de la Gobernación de Norte de Santander.
- Solucionar contingencias presentadas ante el surgimiento de virus o malware que la solución no se haya detectado automáticamente.
- Configurar el analizador de red para la detección de virus o malware.
- La Secretaría TIC aislará el equipo o red, notificando a la Secretaria, oficina o alta consejería correspondiente, en las condiciones siguientes:
  - ✓ Cuando la contingencia con virus o malware no es controlada, con el fin de evitar la propagación del virus o malware a otros equipos y redes.
  - ✓ Si el usuario viola las políticas antivirus o antimalware.
  - ✓ Cada vez que los usuarios requieran hacer uso de discos, USB's, o cualquier dispositivo de almacenamiento éstos serán rastreados por la Solución Antivirus o antimalware en la computadora del usuario o en un equipo designado para tal efecto en la Secretaría TIC.

USO DEL ANTIVIRUS POR LOS USUARIOS

- El servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus o malware.
- Si el servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus o antimalware en la computadora del usuario o por el equipo designado para tal efecto.
- El servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) deberá comunicarse con la Secretaria TIC en caso de problemas de virus o malware para buscar la solución.
- El servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) será notificado por la Secretaria TIC en los siguientes casos:

  - ✓ Cuando sea desconectado de la red con el fin evitar la propagación del virus o malware a otros usuarios de la secretaria, oficina o altas consejerías.
  - ✓ Cuando sus archivos resulten con daños irreparables por causa de virus o malware.
  - ✓ Cuando viole las políticas antivirus o antimalware.

SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles.

Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros. La Secretaría TIC implementará soluciones lógicas y físicas que garanticen la protección de la información de la Gobernación de Norte de Santander de posibles ataques internos o externos.

- ✓ Rechazar conexiones a servicios comprometidos
- ✓ Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).

- ✓ Proporcionar un único punto de interconexión con el exterior.
- ✓ Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- ✓ Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- ✓ Auditar el tráfico entre el exterior y el interior.
- ✓ Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos.

FIREWALL

- La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.
- Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
- La Secretaría TIC establecerá las reglas en el Firewall necesarias para bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- El firewall debe bloquear las "conexiones extrañas" y no dejarlas pasar para que no causen problemas.
- El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
- Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

CONECTIVIDAD A INTERNET

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) de la Gobernación de Norte de Santander tienen las mismas responsabilidades en cuanto al uso de Internet.

- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
- No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.
- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.
- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

RED INALAMBRICA (WIFI)

Acceso

- La red inalámbrica es un servicio que permite conectarse a la red de la Gobernación e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de la Gobernación.
- Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
- Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Tablets, celulares, etc.) con capacidad de conexión Wireless.
- La Secretaría TIC, es la dependencia encargada de la administración, habilitación y/o bajas de usuarios en la red inalámbrica de la Gobernación de Norte de Santander.

Identificación y activación

- Para hacer uso de la red inalámbrica, el solicitante necesariamente debe ser servidor público (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) de la Gobernación de Norte de Santander.
- Como primer paso para hacer uso de este servicio, se deben de registrar los usuarios que deseen la prestación del servicio mediante el llenado de un formulario y presentando el dispositivo que se conectará a la red inalámbrica.

- Se debe registrar la dirección MAC de las tarjetas inalámbricas de todos y cada uno de los dispositivos de comunicación.
- La activación de la cuenta se realizará por un periodo semestral como máximo; salvo casos de fuerza mayor o anormalidades en el registro (usuarios inexistentes, apagones, fallas, etc.).
- Para conectarse a la red inalámbrica se deberá emplear autenticación tipo WPA2 para lo cual la contraseñas cambiarán periódicamente (de 6 a 12 meses) con la finalidad de proporcionarles seguridad en el acceso a los funcionarios (Planta, Contratista).

Seguridad

- A pesar de que se han establecido sistemas de encriptación de datos mediante el uso de seguridad WPA2, NO SE RECOMIENDA hacer uso de tarjetas de crédito para compras.
- La Secretaria TIC determinará las medidas pertinentes de seguridad para usar las redes inalámbricas.
- La Secretaria TIC se reserva el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red. No se deben realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de ingreso no autorizado es una práctica ilegal y será analizada para su respectiva sanción.
- No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.
- Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar a la Secretaria TIC para su respectiva baja del equipo de la red inalámbrica.

Tecnología

- La red inalámbrica de la Gobernación de Norte de Santander usa tipo estándar con cifrado WPA2. Por lo tanto las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi™ de este estándar y soportar los requerimientos descritos. Caso contrario se debe realizar algunas actualizaciones previas de tratarse de un computador portátil.

- A pesar de que se usan amplificadores de señal, la cobertura queda sujeta a diversos factores, por lo que NO SE GARANTIZA en ninguna forma el acceso desde cualquier punto fuera de cobertura de la Gobernación.
- Sólo será soportado el protocolo TCP/IPV.4 (Por Ahora) en la red inalámbrica.
- La Secretaria TIC se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los funcionarios (Planta, Contratista) de la Gobernación de Norte de Santander.
- No se permiten la operación ni instalación de "puntos de acceso" (access points) conectados a la red cableada de la Gobernación de Norte de Santander sin la debida autorización por parte la Secretaria TIC.
- No se permite configurar las tarjetas inalámbricas como "puntos de acceso" o la configuración de equipos como servidores adicionales.

RESTRICCIONES Y/O PROHIBICIONES DE ACCESO A INTERNET

- El uso de programas para compartir archivos (Peer to Peer).
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- El uso de sitios de videos en línea o en tiempo real.
- Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
- Uso de JUEGOS "on line" en la red.

Excepciones

- Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.
- En caso de eventos, cursos, talleres, conferencias, etc, se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.
- En el caso de estos eventos las restricciones para acceder podrán ser "anuladas" temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.

Acceso a Invitados

- La red inalámbrica (WIFI_PALACIO) es un servicio que permite conectarse única y exclusivamente a personal externo de la Gobernación de Norte de Santander (ciudadanos, clientes, proveedores) a internet sin la necesidad de algún tipo de cableado. La Red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura de la Gobernación.
- Los usuarios invitados no tendrán acceso a la Red de la Gobernación ni a ningún recurso de uso privado de la Gobernación.

PLAN DE CONTINGENCIAS TECNOLOGICAS

La Secretaria TIC creará para las secretarías y oficinas un plan de contingencias tecnológicas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos tecnológicos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, la Gobernación de Norte de Santander se reserva el

derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los funcionarios (Planta, Contratista) de la Gobernación.

Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de la Política de Seguridad de la Información.

Disposiciones

- Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.
- Las normas y políticas objeto de este documento podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo de la Secretaría TIC; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.
- La falta de conocimiento de las normas aquí descritas por parte de los servidores públicos (Gobernador, Secretarios, Altos Concejeros, Jefes de Oficina, Funcionarios de Planta y Contratista) no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

WILLIAM VILLAMIZAR LAGUADO
Gobernador del Departamento de Norte de Santander

MARINA LOZANO ROPERO
Secretaría de Tecnologías de la Información y Comunicaciones

CHRISTIAN ALFONSO SARAVIA URIBE
Ingeniero de Sistemas – Secretaría de las TIC