POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Seguridad y Privacidad de la Información
Dimensión: Diagnóstico de Seguridad y Privacidad

Gobierno Digital

Ministerio de las Tecnologías de la Información y Comunicaciones

Alcaldía de Oiba

2018

Contenido

Histórico

VERSIÓN	FECHA	AUTOR
1	01-11-2016	Secretaría de Gobierno
2	01-12-2017	Secretaría General y de Gobierno
3	01-06-2018	Secretaría General y de Gobierno

Introducción

Esta política se construye siguiendo los lineamientos de la Guía del dominio de Estrategia: Definición y diseño de una política de TI – Guía técnica Versión 1.0 publicada el 26 de mayo de 2015, la cual fue elaborada por el Ministerio de las Tecnologías de la Información y Comunicaciones (MinTIC) y su autora fue la Viceministra de Tecnologías y Sistemas de la Información, María Isabel Mejía Jaramillo.

De acuerdo al esquema de fortalecimiento de la gestión TI en el Estado, de MINTC, una política TI se elabora con el fin de aumentar la productividad, flexibilidad y dinámica del Estado en cuanto a TI, las entidades deben actuar en conjunto con ayuda de lineamientos, guías y estándares que les faciliten la gestión de sus recursos y proyectos, y conlleven a resultados más eficientes. Un grupo de expertos ha venido desarrollando dichos documentos, de tal manera que los diversos actores del sector TI tengan unos caminos de guía para llevar a cabo cualquier proceso de TI en el sector público o privado. Los siguientes son los temas que serán regularizados por medio de lineamientos, estándares y guías. Los documentos serán publicados una vez se legalicen y oficialicen.

Además se consultó como guía de caso de uso el Manual de la Política de Seguridad para las Tecnologías de la Información y las Comunicaciones – TIC del Departamento Administrativo de la Presidencia de la República, publicada en Mayo de 2016

1. Objetivo

Definir los lineamientos relacionados con la Seguridad y Privacidad de la Información de la Alcaldía del Municipio de Oiba en Santander.

2. Alcance

Esta política tiene como fin ser aplicada en todas las tareas, servicios o trámites a ejecutar en la entidad, a su vez se busca el cumplimiento de la misma por parte de los funcionarios, contratistas y organizaciones relacionadas (de ahora en adelante usuarios) con la Alcaldía del Municipio de Oiba en Santander. Esto tiene como finalidad garantizar la idoneidad, protección y confianza en el uso de los bienes y servicios informáticos de la institución, siempre y cuando el compromiso de los usuarios sea el mejor con relación al cumplimento de la misma.

Cómo lo indica en su Plan de Desarrollo Municipal (2016-2019) en el año 2025 el municipio será un territorio reconocido a nivel nacional como pionero en la reducción de brechas sociales, equitativo, transparente, laborioso y respetuoso, que sustenta su sostenibilidad en la innovación constante de sus procesos productivos representados en el sector agropecuario y turístico, y de dialogo permanente y abierto entre la ciudadanía y la administración, para la búsqueda de una paz duradera y el respeto de los derechos humanos con enfoque en la Primera Infancia, la Infancia, la Adolescencia, la Familia y la Mujer.

Uno de sus objetivos principales en su dimensión institucional es la de garantizar la participación de los Oibanos en el desarrollo del ejercicio público.

3. Marco legal

- Decreto 1078 de 2015 - Decreto Único Sectorial - Lineamientos generales de la Estrategia de Gobierno en Línea
- Decreto 235 de 2010 - Intercambio de información entre entidades para el cumplimiento de funciones públicas
- Guía técnica G.ES.03 - Guía del dominio de Estrategia: Definición y diseño de una política de TI
- Norma Técnica ISO-IEC 270012013 estándar para la seguridad de la información

4. Términos y definiciones

Activos de información: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos usuarios, contraseñas, números de cuentas, etc.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le Permitan emitir un juicio informado sobre el estado y efectividad del sistema de gestión de la seguridad de la información de una organización.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido,

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Gusanos: Es un programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

Ingeniería Social: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del

sistema de gestión de la seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Keyloggers: Aplicaciones que registran el teclado efectuado por un usuario.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas. Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Seguridad de la información: La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser electrónicos, en papel, audio, vídeo y otros multimedia.

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIlEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5. Política general de seguridad y privacidad de la información

La dirección de la Alcaldía Municipal de Oiba, 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 Alcaldía Municipal de Oiba, 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 Entidad según como se defina en el alcance, sus funcionarios, 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 sus clientes, socios y empleados.
- 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 funcionarios, terceros, aprendices, practicantes y clientes de la Alcaldía Municipal de Oiba
- Garantizar la continuidad del negocio frente a incidentes.
- La Alcaldía Municipal de Oiba 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.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la

información" y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación se establecen 12 principios de seguridad que soportan el SGSI de la Alcaldía Municipal de Oiba:

- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, socios de negocio o terceros.**
- La Alcaldía Municipal de Oiba **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 clientes), o como resultado de un servicio interno en outsourcing.
- La Alcaldía Municipal de Oiba **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 Alcaldía Municipal de Oiba **protegerá su información** de las amenazas originadas por parte **del personal.**
- La Alcaldía Municipal de Oiba **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos.**
- La Alcaldía Municipal de Oiba **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Alcaldía Municipal de Oiba **implementará control de acceso** a la información, sistemas y recursos de red.
- La Alcaldía Municipal de Oiba garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Alcaldía Municipal de Oiba 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 Alcaldía Municipal de Oiba **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Alcaldía Municipal de Oiba garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

6. Políticas

Las políticas que se presentarán a continuación se conforman con una misma estructura: objetivo, aplicabilidad y directrices. La finalidad de estas políticas es que sirvan como herramientas para le entidad no solamente como parámetros de trabajo sino como

mecanismos de sensibilización respecto a la seguridad de la información a los usuarios de la alcaldía, para que así los diferentes procesos de interacción se logren de forma segura, idónea y eficaz.

6.1 Política general de seguridad de la información

Objetivo	Establecer los requisitos generales y necesarios que permitan dar seguridad a la información de la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus bienes o servicios informáticos

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Supervisar el ciclo de vida las políticas de seguridad, es decir; definir, implementar, revisar, auditar y actualizar, las políticas de acuerdo a la implementación de esta y la actualización normativa relacionada, así como las necesidades que presenten los usuarios de la entidad
2. Debido a que la entidad no cuenta con un área de tecnologías, el asesor en tecnologías de la entidad junto con la Secretaría de General y de Gobierno, Almacén Municipal y Secretaría de Hacienda, deben supervisar y seleccionar los bienes y/o servicios tecnológicos que proyecte adquirir la institución

6.2 Organización de la seguridad de la información

Objetivo	Establecer el comité directivo de la seguridad de la información	**Aplicabilidad**	Alcalde, Secretarios de despacho, y otros funcionarios

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. El comité directivo se conforma por

    a. El alcalde o alcaldesa municipal
    b. La/el Secretaria(o) de General y de Gobierno
    c. La/el Secretaria(o) de Hacienda
    d. La/el Secretaria(o) de Planeación y Obras Públicas
    e. El/la Secretaria de Tránsito
    f. Almacenista
    g. Funcionario con responsabilidad en los temas de TIC
2. El comité debe velar por el mejoramiento continúo de los programas o las

6.2 Organización de la seguridad de la información

distintas actividades que se realizarán en este comité
3. Verificar el avance de los distintos proyectos relacionados con esta política
4. Revisar el documento de la política de seguridad
5. Velar por el cumplimiento de las políticas establecidas en este documento

6.3 Política de gestión de activos

Objetivo	Indicar los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de información	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus activos de información

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Se realizará al menos dos veces en el año procesos de identificación y/o actualización del inventario de activos de información por cada una de las dependencias en las cuales los secretarios de despacho serán los responsables de dichos activos de información.
2. Todo activo de información será clasificado de acuerdo a la criticidad, sensibilidad y reserva establecido por la entidad conforme a las leyes como Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015.
3. Los activos de información se deben etiquetar y/o rotular bajo la responsabilidad de cada uno de los secretarios de despacho con el acompañamiento de personal experto.
4. Los funcionarios, contratistas y/o terceros deben realizar la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad.
5. Con relación a los medios removibles todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores, los cuales serán autorizados para compartir información autorizada con personal externo a la entidad, siempre y cuando el líder del área de tecnologías y seguridad de la información lo autorice
6. Es obligatorio realizar de forma segura y correcta la eliminación, retiro, traslado o re uso cuando no se requieran los activos de información. Por lo cual es relevante realizar backups los cuales se evien el el acceso o borrado no autorizado.

6.4 Política de control de acceso

Objetivo	Determinar la protección, límites y procedimientos	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y

	frente a la administración y responsabilidad, relacionados con los acesos a la inofrmación.		demás potenciales usuarios que tengan relación con la entidad y sus activos de información

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. El acceso a redes, aplicaciones y/o sistemas de información de la entidad se debe hacer mediante usuarios y contraseñas, y asignadas a cada funcionario el cual es responsable del uso de estas
2. La gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios de los usuarios asignados será administrada por el encargado de TI de la entidad
3. La calidad de las contraseñas constará de al menos 8 caracteres las cuales contendrá caracteres alfa numéricos y especiales.

6.5 Política de no repudio

Objetivo	Evitar acciones de repudio por parte de los usuarios	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus activos de información

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Realizar seguimiento a la creación, origen, recepción y entrega de información
2. Tener logs de registro de las acciones realizadas por los usuarios, la cual será informada a los usuarios
3. Realizar auditorías continuas, como procedimiento para asegurarse que las partes implicadas se nieguen haber realizado una acción
4. Los servicios de intercambio electrónico de información son garantía de no repudio

6.6 Política clasificación de la información

Objetivo	Brindar un nivel de protección apropiado a la información que produce o hace uso la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y la

			información que estos generen o hagan uso de la entidad

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. En la entidad se considera como información:
    a. Comunicados o mensajes que son transmitidos de forma oral ya sea personalmente o por medios electrónicos como llamadas de voz, video llamadas entre otras
    b. Comunicados o mensajes que son transmitidos de forma escrita ya sea por medios electrónicos como medios magnéticos, físicos, herramientas de mensajería, entre otros.
    c. Formularios, encuestas y otros mecanismos de captura de información propios o de terceros, ya sea por mecanismos virtuales o físicos
    d. Información almacenada o generada en los equipos, sistemas o servicios informáticos, medios magnéticos/electrónicos y/o medios físicos
2. Es responsabilidad del usuario identificar los posibles riesgos a los que puede ser expuesta la información que utiliza ya que esta puede ser copiada, divulgada, alterada o eliminada ya sea de forma física o digital a manos de funcionarios o personal externo de la entidad
3. El funcionario debe seguir los lineamientos de los activos de información de la entidad para lograr la identificación y administración óptima de estos

6.7 Política seguridad en el papel del talento humano

Objetivo	Reducir el riesgo de uso no adecuado de la información por parte de los usuarios de los bienes y servicios informáticos de la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus bienes o servicios informáticos

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Los usuarios deben entender las responsabilidades de sus cargos o funciones con las políticas de seguridad de la información de la entidad para así disminuir el riesgo del uso no adecuado, pérdida, hurto, fraude o filtración de la información en los bienes y servicios informáticos utilizados de la entidad
2. Se recomienda al usuario crear una cuenta con su correo electrónico institucional en herramientas de servicio de almacenamiento en la nube tales como Dropbox, Drive u Outlook, para que pueda tener un respaldo de se seguridad de su información en caso de daños al equipo. Sobre esta cuenta tendrá conocimiento la administración municipal y las oficinas encargas del área de TI

6.7 Política seguridad en el papel del talento humano

3. Los programas que se instalarán en las estaciones de trabajo (equipos de cómputo y Smartphone) deben cumplir con dos características: 1. Licenciandos (legales) y 2. Autorizados por las personas encargadas de Tecnologías de Información en la entidad, no se permite el uso de software que no cumpla con esas condiciones
4. Las herramientas software de la entidad deben tener su respectiva licencia y cumplir con lo acordado por los derechos de autor
5. Las herramientas instaladas sin autorización del área de TI en la entidad deben ser eliminadas ya que esto expone a posibles ataques informáticos en la entidad
6. Buscando agilidad y seguridad de la información, todo dispositivo de almacenamiento externo al equipo de trabajo de cómputo tales como memorias Flash USB, DVD, CD, Dispositivos móviles, entre otros, serán analizados automáticamente por una plataforma de antivirus, a menos que el Sistema Operativo en uso represente una seguridad tal que no necesite la instalación de software antivirus
7. Las herramientas software instaladas en los equipos de cómputo de la entidad son propiedad de esta. En el caso que sean aplicativos de entidades de orden nacional estos pertenecerán a sus distribuidores y la entidad tendrá tan solo derechos de uso, por lo tanto las licencias o las mismas herramientas software no pueden ser copiadas
8. La entidad puede realizar auditorías anunciadas y no anunciadas con la finalidad de mantener la integridad institucional con el fin de identificar copias no autorizadas de programas o herramientas en los equipos de cómputo en la entidad
9. Los bienes y servicios tecnológicos asignados a cada usuario de la entidad son responsabilidad de dicho usuario
10. Debido a la responsabilidad de cada usuario sobre los bienes y servicios informáticos asignados este debe abstenerse de almacenar en ellos información que no sea de carácter institucional, de acuerdo a los parámetros de activos de información
11. La información no autorizada para su divulgación por parte de los usuarios de la entidad acarreará responsabilidades disciplinarias y legales
12. Los bienes y servicios tecnológicos de la entidad deben ser utilizados únicamente para el propósito que estos fueron adquiridos
13. Antes la presencia de eventos que el usuario considere que pueden debilitar o comprometer la seguridad de la información en la entidad, se debe reportar a las personas encargadas del área de TI de la entidad
14. Con el apoyo de los secretarios de despacho y el alcalde municipal se socializarán una serie de lineamientos a tener en cuenta al momento de compartir información reservada de la entidad como contraseñas de acceso a diferentes servicios informáticos y otra información de carácter confidencial a través de medios de comunicación virtuales o presenciales tales como: llamadas telefónicas, aplicaciones de mensajería, o conversaciones presenciales
15. Para compartir información entre una usuario y otro es mejor utilizar medios de comunicación auditados como el correo electrónico o la intranet

6.8 Políticas para funcionarios y contratistas del Área de Tecnologías y Sistemas de Información

Objetivo	Establecer los lineamientos que garanticen la seguridad de la información de la entidad por parte de los funcionarios y contratistas de TI	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. El personal del área de TI no debe dar a conocer contraseñas de acceso a terceros sin previa autorización de la persona líder del Área de TI
2. Los usuarios y claves de acceso de los administradores de sistemas y del personal del Área de TI son información de uso personal e intransferible
3. El Área de TI debe emplear el uso de contraseñas de alto nivel de complejidad, autenticación en dos vías para el acceso a servicios TI que administren usuarios o herramientas en la entidad
4. La información de procedimientos, seriales, software entre otros deben mantenerse bajo custodia para evitar el acceso a personas no autorizadas
5. Cuando se realice el cambio o retiro de equipos de los funcionarios o usuarios de la entidad, es necesario seguir políticas de saneamiento, es decir, prácticas que mejoren la eliminación de la información contenida, a través de un formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos
6. El personal de TI encargado de realizar instalaciones de software en los equipos de cómputo de la entidad, instalará herramientas licenciadas y/o legales autorizados
7. Sin la autorización correspondiente los encargados del Área de TI no debe otorgar permisos especiales a los usuarios de los diferentes bienes o servicios tecnológicos de la entidad
8. Los encargados del Área de TI no utilizará la información para fines comerciales o diferentes al ejercicio de sus funciones
9. Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
10. Todo bien o servicio informático y sus medios, deben ser únicamente instalados en los equipos y servidores de la entidad, donde a su vez se deben hacer copias de seguridad de acuerdo con las políticas del proveedor y de la entidad
11. Deben ser bloqueados los protocolos y servicios que no se requieren en los equipos de cómputo de la entidad, a menos que sean solicitados y aprobados oficialmente por la entidad a través del Área de TI.
12. El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado

6.9 Políticas para el/la Administrador del sitio web			
Objetivo	Mantener la integridad del sitio Web Institucional, software o aplicativos e información contenida	**Aplicabilidad**	Las personas encargadas de la actualización y soporte del sitio web de la entidad
Directrices			

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Las personas encargadas de la actualización y soporte del sitio web de la entidad deben apegarse a la seguir la Política Editorial y Actualización de Contenidos Web, así como los lineamientos de la estrategia Gobierno en Línea
2. Las claves de acceso al administrador del Sitio web institucional de la entidad son estrictamente confidenciales, personales e intransferibles

6.10 Política de disponibilidad de información, medios y equipos			
Objetivo	Disponer de un funcionamiento óptimo de los equipos, información y distintos medios tecnológicos ante posibles fallas o desastres en la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Los medios y equipos donde se almacene, procese o comparta información, deben contar con lineamientos de protección física y lógica
2. Realizar monitoreo sobre el estado del funcionamiento de los medios y equipos de información
3. Realizar mantenimientos preventivos y correctivos pertinentes

6.11 Política de rintegridad, espaldo y restauración de información			
Objetivo	Establecer mecanismos de respaldo adecuados para conservar la información y software antes posibles fallas	**Aplicabilidad**	Personal encargado de administrar los bienes y servicios de TI en la entidad
Directrices			

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Almacenar de forma regular la información de los equipos en medios magnéticos como CD, DVD, Cartucho, Cinta, etc...
2. El funcionario o asesor encargado de coordinar el uso de bienes y servicios de TI debe establecer la frecuencia con la cual se realicen respaldo a estos activos de información
3. Las copias de información importantes deben almacenarse en un lugar que garantice la integridad de la información almacenada
4. La finalidad de guardar copias de respaldo es que se utilizarán únicamente cuando el sistema o área de trabajo deba ser reestablecida debido a daños de hardware o software, o por requerimiento legal
5. Se debe mantener un inventario actualizado de los respaldos realizados a los diferentes equipos o sistemas informáticos

6.12 Política de uso de estaciones de trabajo

Objetivo	Garantizar la seguridad y buen uso de las estaciones de trabajo de la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. La instalación de software en los computadores de las dependencias es una función que puede realizar solamente el Área de TI de la entidad, además de dispondrá en una lista actualizada del software autorizado para instalar en los computadores
2. La unidad de almacenamiento de cada estación de trabajo deberá estar dividida en al menos dos discos virtuales (C: y D:) donde el disco C: contendrá el sistema operativo y software para las labores del funcionario, mientras que el disco D: contendrá los archivos o información generada por el funcionario, esto con el fin de mejorar el nivel de integridad de la información, a menos que se cuente un Sistema Operativo Linux, el cual garantiza la integridad de la información independiente de sus archivos de S.O
3. Las terminales de trabajo (computadores de escritorio) no pueden salir de la entidad o ser llevadas de una oficina a otra a menos que lo autorice y supervise el Área de TI, en el caso de los equipos portátiles que pertenezcan a la entidad pueden ser transportados libremente dentro la entidad siempre y cuando por la persona responsable del equipo, pero no deben salir de la institución, a menos que el Área de TI lo autorice, además debe llevarse un registro de salida y entrada de equipos debidamente firmado por cada funcionario
4. Cuando un usuario quiera prestar un equipo que está bajo su responsabilidad a otro usuario dentro la entidad debe solicitar autorización al Área de TI y dejar registro del préstamo realizado donde los dos usuarios firmen la entrega y

6.12 Política de uso de estaciones de trabajo
recibido del mismo

6.13 Política de uso Internet			
Objetivo	Definir los lineamientos que establezcan una navegación segura y uso adecuado de la red de la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 01-06-2018 **Política autorizada por:** Maria Lucila Sarmiento Aguilar **Quiénes pueden brindar información:** Secretaría General y de Gobierno 1. La navegación en internet debe realizarse con propósitos labores o que busquen mejorar el rendimiento laboral y personal de los usuarios de la entidad 2. No es permitida la navegación en sitios con contenidos contrarios a la ley o políticas de la entidad, los cuales puedan presentar riesgos tales como: pornografía, terrorismo, hacktivismo, segregación o discriminación racial, entre otros que puedan atentar con la integridad de la entidad y su misión y visión 3. En caso de acceder a este tipo de contenidos con fines de investigación o seguridad, se debe contar con la autorización del Área de TI 4. La descarga de archivos de internet debe ser con fines laborales y de manera coherente al uso común de la misma, es decir no se deben realizar con regularidad descargas que afecten el ancho de banda de la red ya que limita el uso de la misma a los demás funcionarios en la entidad, en caso de realizar descargas de mayores a 400 Mbs se recomienda hacerlas en horarios no laborables, dejando que el equipo realice el proceso de forma automática		

6.14 Política de mensajería instantánea y redes sociales			
Objetivo	Definir lineamientos para el uso de servicios de mensajería instantánea y redes sociales para usuario autorizados	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios **autorizados** que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 01-06-2018 **Política autorizada por:** Maria Lucila Sarmiento Aguilar **Quiénes pueden brindar información:** Secretaría General y de Gobierno 1. El uso de mensajería instantánea y acceso a redes sociales por medios de los bienes y/o servicios informáticos de la entidad debe ser realizado únicamente por los **usuarios autorizados** por el Área de TI			

6.14 Política de mensajería instantánea y redes sociales

2. Todo usuario que no esté autorizado para hacer uso de redes sociales y herramientas de mensajería instantánea con los bienes y/o servicios informáticos de la entidad debe abstenerse de hacer uso de estas
3. No se permite el envío de mensajes con contenido que atente con la integridad de la comunidad en general o instituciones al igual se prohíbe material que pueda contener o llevar a lugares con código malicioso
4. La información que se publique en redes sociales o por medio de herramientas de mensajería instantánea a nombre personal es considerada fuera del alcance del Área de TI de la entidad y la entidad misma, y por lo tanto su fidelidad, coherencia, confiabilidad, integridad y disponibilidad y los potenciales daños o perjurios causados o que puedan causar son responsabilidad explicita de la persona que haya producido esta tipo de contenido

6.15 Política de uso de impresoras y servicio de impresión

Objetivo	Fomentar una correcta operación e integridad de las impresoras y servicios de impresión en la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. El uso de los dispositivos de impresión deben alinearse principalmente a la política de cero papel de la entidad
2. Los documentos que se impriman en la entidad deben ser de carácter institucional y laboral
3. El usuario debe dar un correcto uso a los equipos de impresión que están a su cargo para evitar el posible daño de estos
4. Se recomienda a los usuarios no realizar labores de reparación o mantenimiento de las impresoras, específicamente en sus características de hardware, en caso de presentarse alguna falla debe contactarse el área de TI de la entidad

6.16 Política de uso de puntos de acceso a las redes LAN y Wi-fi

Objetivo	Coordinar un uso correcto de los puntos de acceso a la red, intranet e internet	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 01-06-2018

6.16 Política de uso de puntos de acceso a las redes LAN y Wi-fi

Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Los equipos de trabajo de la entidad se deben conectar a la red por medio de puntos LAN, red cableada, esto con el propósito de estabilidad y seguridad de la información
2. Los usuarios como contratistas, invitados y entre otros que no son funcionarios de planta en la entidad, deben conectar sus terminales a las redes wi-fi puestas a disposición en la entidad. El acceso a estas redes deben ser autorizadas y configuradas por el Área de TI
3. La activación, gestión y uso de los punto de red en la entidad es responsabilidad el Área de TI

6.17 Política de seguridad de los Equipos

Objetivo	Asegurar la idoneidad de la información almacenada en los equipos	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. El suministro de energía de los equipos en caso de no ser regulada, debe contar al menos cada equipo con un dispositivo tal como un estabilizador y en el caso que sea posible una UPS
2. El cableado debe estar marcado para identificar los elementos conectados y evitar desconexiones erróneas
3. Es necesario realizar soporte y mantenimiento a los equipos, por lo tanto es recomendable tener contratos de soporte tanto preventivo como correctivo
4. Es necesario llevar registro de las acciones de soporte y mantenimiento realizadas a los equipos de la entidad
5. En caso que un equipo deba ser retirado de la entidad y trasladado a laboratorios u organizaciones de soporte y mantenimiento de equipos informáticos es necesaria la autorización y registro de la salida y enredada de estos
6. El ingreso y retiro de todo activo de información en la entidad debe ser registrado y autorizado por el Área de TI

6.18 Política de escritorio y pantalla limpia

Objetivo	Definir los lineamientos para reducir el riesgo de acceso no autorizado, pérdida y daño de	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que

6.18 Política de escritorio y pantalla limpia			
	información		tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. El escritorio del equipo de trabajo del usuario debe estar libre de información para que esta no pueda ser copiada o eliminada fácilmente por otros usuarios o terceros sin autorización, además de facilitar el soporte del terminal
2. La pantalla se debe bloquear toda vez que el usuario no esté en su estación de trabajo, para lo cual es recomendable establecer contraseña al usuario con el que se inicia sesión
3. Al imprimir documentos de tipo confidencial, estos deben ser retirados inmediatamente de la impresora

6.19 Política de uso del correo electrónico			
Objetivo	Definir lineamientos para asegurar la protección de la información de la entidad en el uso de correo electrónico	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, y usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Los usuarios de correo electrónico corporativo (institucional) son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información
2. El acceso al correo electrónico se realizará de forma local en el equipo asignado a cada funcionario, a través de herramientas administradoras de correo electrónico instaladas en el equipo de trabajo
3. La finalidad del uso de correo electrónico es de carácter operativo, laboral e institucional
4. No se debe utilizar este correo para fines personales o compartir información personal
5. No está permitido el envío de cadenas o correos masivos que no sean de tipo laboral
6. Se debe procurar evitar el envío de correos electrónicos con un peso superior a las 20 MB
7. No está permitido el envío de correos que atenten contra la integridad y dignidad de las personas o que puedan dañar su buen nombre
8. Cuando un funcionario se retire de su cargo el correo continuará vigente y entrará

6.19 Política de uso del correo electrónico

en funcionamiento al nuevo funcionario asignado

9. El tamaño del correo electrónico está en función de la capacidad del equipo de trabajo donde este se encuentre instalado
10. Se creó una cuenta de correo electrónico en la web donde se reenviarán todos los correos recibidos en las cuentas institucionales que servirá como Backup
11. Las cuentas de correo no son propiedad del funcionario o usuario, son propiedad del sistema de administración web el cual presta el servicio en la entidad
12. El usuario es responsable de la información y archivos adjuntos que se envían desde la cuenta de correo asignada
13. Todo mensaje que el usuario considere sospechoso debe ser reenviado a la cuenta de correo contactenos@oiba-santander.gov.co para realizar su análisis, además este correo sospechoso debe ser eliminado y no abrir ningún enlace o archivo adjunto contenido en el mismo

6.20 Política de uso de la red intranet

Objetivo	Definir lineamientos para hacer buen uso de la red intranet de la entidad	**Aplicabilidad**	Todos los funcionarios que hagan uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Los usuarios conectados a la red interna (intranet) por medio de conexión cableada serán los autorizados para hacer uso de esta
2. La intranet les permitirá compartir archivos entre funcionarios con una velocidad de 100Mb/s lo que representaría una horro en el ancho de banda de internet
3. Además podrán realizar Backups en el servidor central, con un tamaño máximo de 10Gb por usuario
4. No se permite el uso de la intranet para realizar tareas personales o compartir archivos que no estén relacionados con las labores o funciones de la institución

6.21 Política de uso servicio de mensajería Empathy

Objetivo	Definir lineamientos para hacer buen uso del servicio de mensajería	**Aplicabilidad**	Todos los funcionarios que hagan uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 01-06-2018
Política autorizada por: Maria Lucila Sarmiento Aguilar
Quiénes pueden brindar información: Secretaría General y de Gobierno

1. Este servicio tiene con finalidad facilitar la comunicación con fines laborales

entre funcionarios
2. Se recomienda hacer un buen uso del lenguaje, respetando la integridad de los demás funcionarios
3. Este servicio será auditado, así que está prohibido eliminar las conversaciones entre funcionarios

7. Procedimientos

Los procedimientos son la descripción de la forma detalladas sobre las actividades necesarias en la realización de un proceso, los procedimientos listados siguen las normas de los lineamientos de acuerdo a la correspondencia y vínculos técnicos entre las normas NTCGP1000 y NTC-IS09001 y las normas NTC-IS09001 y NTC-IS027001.

- Procedimiento de control de registros
- Procedimiento de auditoría interna
- Procedimiento de acción correctiva
- Procedimiento de acción preventiva
- Procedimiento de revisión del Manual de la Política de Seguridad

8. Proceso disciplinario

A continuación se presenta el listado de acciones que pueden llevar al usuario a cometer faltas de tipo disciplinario y a su vez violar los procedimientos de seguridad de la información:

- No participar en la socialización de los lineamientos y acuerdos de confidencialidad sobre el uso y entrega de los activos de información
- Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización y no reportarlo al Área de TI de la entidad
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello
- No actualizar la información de los activos de información a su cargo
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, de documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)

- Dejar información pública reservada, en carpetas compartidas
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios
- Dejar los computadores encendidos en horas no laborables, a menos que el Área de TI solicite lo contrario
- Permitir que personas ajenas a la entidad, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad
- Solicitar cambio de contraseña de un usuario distinto al otorgado al funcionario, sin la debida autorización del titular o su jefe inmediato
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (exceptuando el penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional, tanto de los bienes o servicios informáticos
- Compartir correos electrónicos no institucionales para recibir o enviar información laboral de la entidad
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación
- Utilizar equipos electrónicos o tecnológicos desatendidos o que a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área de TI de la entidad
- Permitir el acceso a particulares o terceros a los servicios o bienes tecnológicos asignados a cada usuario sin la autorización del Área de TI
- Uso de servicios disponibles a través de internet que no estén permitidos por el Área de TI tanto como acceso FTP, Telnet, protocolos y servicios los cuales pueden generar riesgo a la entidad
- Mal uso de los equipos de escritorio o portátiles, teléfonos inteligentes y otros dispositivos entregados a los usuarios para actividades laborales
- Ocultar, destruir, copiar y/o eliminar de la documentación institucional, o destruirla de forma errónea
- Dejar sin supervisión documentación con información pública reservada o clasificada de la institución
- Copiar o almacenar información pública reservada o clasificada, en dispositivos de almacenamiento tales como: memorias flash USB, computadores portátiles, teléfonos, entre otros dispositivos que permitan el almacenamiento de información digital y que no permanezcan en la institución
- Conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la institución, sin la autorización del Área de TI
- Guardar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos

- Uso de los recursos de la institución como servicios, bienes o espacios en redes sociales o medios web, para el beneficio personal del usuario
- Eliminar, dañar, borrar, o programar el borrado de datos informáticos o de un sistema de información de la institución
- Distribuir, enviar, instalar o permitir el ingreso a software malicioso u otros programas de computación de efectos dañinos en los bienes o servicios informáticos de la entidad
- Alterar o corromper datos personales de las bases de datos de la institución
- Suplantar a un usuario en alguno o todos los sistemas tecnológicos de la entidad
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la entidad o permitir que otras personas accedan con el usuario y clave del responsable a éstos
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la institución a personas no autorizadas
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceder a servicios o bienes informáticos no autorizados de la institución o de terceros
- Llevar a cabo acciones que su propósito o resultado evite o altere los controles de seguridad establecidos en la institución
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización del Área de TI
- Sacar de las instalaciones de la entidad de forma física o virtual, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la entidad, para traslado, reasignación o para disposición final
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la entidad o de alguno de sus funcionarios
- Acceder, almacenar o distribuir pornografía infantil
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Área de TI de la entidad
- Copiar sin autorización los programas de la entidad, o violar los derechos de autor o acuerdos de licenciamiento