POLÍTICA	MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)	**CÓDIGO:**
		VERSIÓN: 1

1. INTRODUCCIÓN	El Instituto Distrital de Turismo de Santa Marta – INDETUR – concibe la información como uno de sus activos más importantes, razón por la cual, entendiendo tal importancia, se ha comprometido con la implementación de la presente política buscando establecer un marco de confianza en el ejercicio de sus labores con sus colaboradores internos y externos, proveedores y/o terceros. La presente política de seguridad y privacidad de la información busca mitigar impactos adversos que puedan afectarla, sean estos físicos o lógicos, con el fin de responder con integridad y confidencialidad, manteniendo la confianza y protegiendo en todo momento los activos tecnológicos, del uso inapropiado, ataques de virus o fuga de información, que comprometan y/o expongan de manera directa al INDETUR. En consecuencia, la política se compone de todos aquellos lineamentos necesarios para la protección de toda su información, entendida como los datos que tienen valor para la empresa y que se hallan soportados tanto física como digitalmente, basados en los principios de confidencialidad, legalidad y seguridad.
2. ALCANCE	La política de seguridad y privacidad de la información será aplicable y debe ser cumplida en su totalidad por todos los funcionarios directivos, coordinadores, gestores, asistenciales, contratistas, proveedores, aliados, y en general, por cualquier tercero que, con ocasión al desarrollo y cumplimiento del objeto social, llegare a tener algún tipo de vínculo comercial o contractual con INDETUR.
3. OBJETIVO GENERAL	Establecer las medidas técnicas, físicas, organizacionales y legales, necesarias para proteger los activos de

	información contra accesos no autorizados; divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso que se pueda producir en forma intencional o accidental.
4. OBJETIVOS ESPECIFICIOS	1. Adoptar, promover e implementar una metodología para la gestión de riesgos para las plataformas tecnológicas como mecanismo único de la entidad para la toma de decisiones, con ello, ejecutar la implementación de contramedida, mitigando los riesgos en las redes y sistemas de información hasta un nivel aceptable por la alta dirección. 2. La información propia sobre la entidad es uno de los activos más importantes a proteger, la cual debe resguardarse con los mecanismos óptimos que preserven la confidencialidad, integridad y disponibilidad de la información. 3. Establecer los mecanismos legales y/o sancionatorios frente a la violación de alguna política de seguridad. 4. Cumplir con los principios de la función administrativa. 5. Apoyar la innovación tecnológica. 6. Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, proveedores, aliados y usuarios. 7. Garantizar la continuidad en la prestación del servicio frente a algún tipo de incidente de seguridad que se llegare a ocurrir.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Cada dirección y/o área de **INDETUR.** encargada de la tenencia, custodia y tratamiento de archivos y datos personales acorde a las acciones que estas generen será la encargada de velar por su adecuado uso acorde al cumplimiento de unos estándares de la política del tratamiento y gestión del riesgo en seguridad de la información, centralizando la implementación y liderazgo en el funcionario de sistemas y medios informáticos de la empresa.

Las políticas que proporcionan principios y guía en aspectos específicos de la seguridad de la información son:

POLÍTICA DE CONTROL DE ACCESO

En **INDETUR** todos y cada uno de los sistemas informáticos y plataformas tecnológicas debe contar con un adecuado control de acceso en:

1. La creación, reactivación o desactivación de usuarios de la red o sistemas de información; al igual que los roles y permisos otorgados, los realizará a través de solicitud enviada por correo electrónico del jefe inmediato y/o supervisor
2. El control para el acceso remoto y redes inalámbricas.
3. Las contraseñas y sistemas de autenticación.
4. El usuario no debe compartir, escribir o revelar su contraseña.
5. Todos los usuarios deben tener una identificación única.
6. Únicamente se debe proporcionar a los colaboradores el acceso a los servicios para los que específicamente se les haya autorizado su uso.

POLÍTICA DE COPIAS DE SEGURIDAD

En **INDETUR** se efectúan copias de seguridad de la información de todas las bases de datos, archivos, aplicaciones, software e información de las unidades de red que se encuentre en los sistemas de almacenamiento y equipos de dentro y fuera de INDETUR. con el fin de garantizar su integridad y disponibilidad.

1. Se debe contar con un sistema automático para la recolección de copias de respaldo.
2. Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.
3. Las bases de datos se encuentran sometidas a protocolos de seguridad que buscan proteger los datos personales frente al acceso no autorizado, adulteración, pérdida, consulta, uso o acceso fraudulento.

POLÍTICA DE ACCESO A INTERNET

En **INDETUR** el uso de la red de internet se destinará exclusivamente a la ejecución de las actividades de la organización y deben ser utilizados por el colaborador para realizar las funciones establecidas para su cargo, por lo cual se definieron los siguientes parámetros para su uso:

1. Los equipos cuentan con protección (firewall) desde y hacia internet para proteger la integridad y confidencialidad de la información.
2. El acceso a internet cuenta con restricciones en la navegación a páginas web.
3. El uso de navegación por internet es a través de páginas HTTPS
4. Se implementaron controles para evitar la descarga de software no autorizado, la infección con código malicioso proveniente de internet y el acceso a sitios catalogados como restringidos y de alta peligrosidad.
5. La descarga de música y videos no es una práctica permitida.
6. El uso inadecuado de internet constituirá una falta grave, que se clasificará como tal por la magnitud del hecho o por no atender los requerimientos de la empresa para que se cese la utilización indebida.

7. Los equipos móviles y de cómputo cuentean con protección para disminuir el riesgo de hurto, destrucción, fluctuaciones de energía, incendio y medio ambiente, utilizando instalaciones en condiciones adecuadas, cerraduras, vigilantes, protectores contra transitorios de energía eléctrica, fuentes de poder interrumpibles (UPS).

POLÍTICA DE CORREO

En **INDETUR** el sistema de correo electrónico es de uso corporativo a través de Zoho mail con dominio propio, en consecuencia, podrá crear, denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado, el uso del correo electrónico deberá ser usado solamente para fines propios a la organización.

1. Los colaboradores que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna en el servidor una vez son vinculados, esta cuenta estará activa durante el tiempo que dure la vinculación del colaborador con la compañía.
2. El sistema de monitoreo filtrará los archivos anexos a los mensajes de correo electrónico, para verificar la ausencia de virus. La entrega de todo mensaje a su destinatario final está sujeta a que esta comprobación sea exitosa.
3. Se prohíbe la utilización de correos electrónicos de dominio diferente al de la compañía para uso de funciones contractuales.
4. Las comunicaciones por correo electrónico entre la entidad y sus públicos de interés deben hacerse a través del correo homologado y proporcionado por la entidad.

POLÍTICA DE MEDIOS EXTRAÍBLES

La utilización no autorizada de memorias o cualquier dispositivo de almacenamiento y transferencia de información física se encuentra restringida a fin de evitar siniestros con la infección de programas malignos y la sustracción de información, archivos y bases de datos de propiedad de **INDETUR.**

POLÍTICA DE DISPOSITIVOS MÓVILES

La información que reposa en los dispositivos móviles asignados por **INDETUR** a cada funcionario, es de responsabilidad de quien tiene en uso el dispositivo móvil. El uso adecuado de los mismos para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas **(VPN),** dependerá de cada funcionario. Cuando se requiera entregar el dispositivo a otro funcionario, la oficina de sistemas y medios informáticos eliminará los datos contenidos en el dispositivo.

POLÍTICA DE SOFTWARE

El hardware, software y periféricos, así como la información en él contenida es propiedad de **INDETUR** y su uso está restringido únicamente para propósitos de la entidad, reservándose el derecho de monitorearlo en cualquier momento.

En cada una de las estaciones de trabajo de **INDETUR** sólo se puede instalar software desarrollado, de uso libre o adquirido legalmente y cuya licencia de uso esté a nombre de **INDETUR.**

1. Las estaciones de trabajo de **INDETUR** deben ser utilizadas por los funcionarios, colaboradores o contratistas sólo para el desarrollo de las

funciones normales de su trabajo. La empresa propenderá por el cambio periódico de los recursos informáticos, dependiendo de la obsolescencia, vida útil, el estado de estos y las necesidades mismas de la entidad, a los cuales, cuando aplique, se les dará de baja.

2. Las cuentas de usuario de herramientas o productos que vengan por omisión se deben deshabilitar inmediatamente después de la instalación de los sistemas o software.
3. Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas o software.
4. Los servidores de archivos, groupware y correo electrónico mantienen activo un software
5. Ninguno usuario puede escribir, distribuir o introducir software que conozca o sospeche que tiene virus.
6. Los computadores de la entidad deberán ser analizados contra virus periódica y automáticamente.
7. Todos los computadores de **INDETUR** deben mantener activo un software antivirus, sistema operativo, servicios de ofimática como Microsoft Office, los cuales están debidamente licenciados y actualizados.

POLÍTICA DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Todos los funcionarios y contratistas de **INDETUR** deben recibir información de sensibilización para tomar conciencia de la seguridad de la información y sus responsabilidades.

Lo anterior, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información en todo momento, razón por la cual, **INDETUR** implementa y adquiere equipos con los controles criptográficos en toda la organización.

1. BITÁCORA

VERSIÓN	FECHA	DESCRIPCIÓN
1	18/03/2022	Administración copias de respaldo

	ELABORADO POR	REVISADO POR	APROBADO POR
NOMBRE	Isnardo Alvarez Polo		Laura Agudelo García
CARGO	Profesional Universitario grado 2, oficina TIC.		Directora General
FIRMA	**(ORIGINAL FIRMADO)**		