POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
Manual de Políticas de Seguridad de la Información para el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones en las Dependencias de la Administración Pública del Estado de Oaxaca.		
CÓDIGO	**FECHA ELABORACIÓN**	**REVISIÓN**
DGTID/DST/MPSI/001	Mayo 2018	3

APROBADO POR	
L.I Eduardo José Herrerías López Director General Dirección General de Tecnologías e Innovación Digital	Ing. Patricia Elena García Herrera Directora de Servicios Tecnológicos Dirección General de Tecnologías e Innovación Digital
ELEBORADO POR	REVISADO POR
Dirección General de Tecnologías e Innovación Digital (DGTID)	M.T.I. Ana Laura Ortega Aguilar Jefa de la Unidad de Planeación y Control de TIC´s

Revisión	Fecha de Revisión	Consideración del Cambio en el Documento
0	Mayo 2018	Creación de Documento
1	Marzo 2019	Se actualizo el nombre del revisor en el campo de revisor Si actualizo el campo 6.0 Revisiones Históricas de la Política agregando nombre y firmas de quien elabora, revisa y aprueba
2	Marzo 2020	• Se incorporó la sección de SEGURIDAD FÍSICA Y AMBIENTAL como parte de las medidas por la pandemia • Se actualiza hacia el concepto a la APE y DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

ÍNDICE

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

POLÍTICA DE SEGURIDAD

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Referencia ISO 27001:2005. A.5 Política de Seguridad. A. 5.1 Directrices de la Dirección General de Tecnologías e Innovación Digital.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento:*** *Programado, en proceso, en revisión y concluido*
A 5.1. A 5.1.1	*Directrices de la Dirección General de Tecnologías e Innovación Digital.* Conjunto de políticas para la seguridad de la información.	2	2.0	Concluido
Vigencia a partir de:		**Marzo 2019**		

Título:

Definición del documento de Políticas de Seguridad de la Información para el uso y aprovechamiento de Tecnologías de la Información y las Comunicaciones en la Administración Pública del Estado de Oaxaca.

Objetivo

Establecer el documento básico de Políticas de Seguridad de la Información para las Dependencias y Entidades del Estado, definiendo los controles para los procesos, normas, métodos, técnicas, configuraciones, tecnologías y/o información y en general sobre el uso y aprovechamiento de Tecnologías de la Información y las Comunicaciones.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

1.0 Propósito

El propósito principal de las políticas de seguridad de la información es informar a los usuarios, grupos de trabajo, y administradores de la plataforma tecnológica del Estado, sobre los requerimientos obligatorios en materia de seguridad informática dictados por la *DIRECCIÓN GENERAL DE TECNOLOGÍAS E INNOVACIÓN DIGITAL* (DGTID), para la protección de la tecnología, la información y sus características. Cada política específica los controles mediante los cuales se cumplirán los requerimientos. Otro propósito es el proveer los lineamientos para ser instalados, configurados y auditados los sistemas computacionales y redes para el cumplimiento de la política.

2.0 Ámbito de Aplicación

Este documento y su contenido aplica para todos los usuarios, administradores y grupos de trabajo que hagan uso y aprovechamiento de las Tecnologías dela Información y las Comunicaciones, en adelante TICs, y para todos y cada uno de los objetos, procesos o procedimientos administrativos tales como: servicios, aplicaciones, accesos físicos y lógicos, protocolos, puertos, dispositivos, interfaces, equipos de comunicaciones y redes, sistemas operativos, programas, sistemas instalados o por instalar en el ámbito de sus funciones, dentro de las instalaciones o complejos administrativos del Estado.

3.0 Política

3.1 Descripción de Política

Los controles de seguridad o la ausencia de ellos son los que, la DGTID como administrador de la plataforma tecnológica del Estado, determinan qué tan seguro o inseguro es cada ámbito y dominio tecnológico. Las metas u objetivos de las políticas de seguridad que ha implementado la *DGTID* se guían por los siguientes criterios:

1.- Servicios requeridos u ofrecidos ***contra*** la seguridad otorgada. Cada servicio que se ofrece a los usuarios conlleva sus propios riesgos de operación. Para algunos servicios, los riesgos sobrepasan los beneficios del servicio y la gestión del riesgo exige elegir entre eliminar el servicio en lugar de tratar de asegurarlo.

2.- Facilidad de uso ***contra*** seguridad. - El sistema más fácil de emplear podría permitir acceso a cualquier usuario sin requerir claves o contraseñas, esto es, prácticamente una seguridad

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

nula. El requerimiento de contraseñas tiene un pequeño inconveniente, pero más seguridad. El empleo de dispositivos para la generación de contraseñas de un solo uso implica mayores inconvenientes para los usuarios, pero es mucho más seguro.

3.- Costo de la seguridad ***contra*** el riesgo de pérdida de información o servicios. – Existen diferentes costos asociados a la seguridad: financiera (por ejemplo, el costo de la compra de dispositivos de seguridad como firewalls, generadores de contraseñas seguras), rendimiento (el cifrado o descifrado toman tiempo adicional), y la facilidad de uso. Hay muchos niveles de riesgo, pérdida de privacidad, pérdida de datos o pérdida de servicios. Cada uno de los costos de servicios debe ser ponderado contra los costos de pérdida de información o de servicios.

Estas metas en materia de seguridad deben ser comunicadas a todo el personal, usuarios, operadores y administradores sobre el conjunto de reglas llamadas “Políticas de Seguridad”. Este término se emplea en lugar del término “Políticas de Seguridad Computacional” debido a que se incluye todo tipo de tecnologías de información y la información almacenada y manipulada por esas tecnologías.

DEFINICIONES

POLÍTICA: Declaración formal y general de principios que presentan la posición de la *Dirección General de Tecnologías e Innovación Digital* para definir su estrategia de control. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías.

Por definición de la *Dirección General de Tecnologías e Innovación Digital*, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir exige que se apruebe una excepción mediante el proceso correspondiente.

ESTÁNDAR: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares definidos por la *Dirección General de Tecnologías e Innovación Digital* son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implementación y promoción de implementación de las políticas de alto nivel de la *Dirección General de Tecnologías e Innovación Digital*, antes de crear nuevas políticas.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

MEJOR PRÁCTICA: Es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la administración de servicios de la *Dirección General de Tecnologías e Innovación Digital*.

GUÍA: Es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas por todos los niveles de operación y de servicios de la *Dirección General de Tecnologías e Innovación Digital*, a menos que existan argumentos documentados y aprobados para no hacerlo.

PROCEDIMIENTO: Definen específicamente las políticas, estándares, mejores prácticas y guías serán implementados en una situación dada dentro de la *Dirección General de Tecnologías e Innovación Digital*. Los procedimientos son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una o toda la organización para implementar la seguridad relacionada a dicho proceso o sistema específico.

Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema. Los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca cómo les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

PERSONAL QUE DEBE ESTAR INVOLUCRADO EN LA FORMACIÓN DE POLÍTICAS DE SEGURIDAD

Con el objeto de que las políticas sean eficaces y apropiadas. Es necesario que cuenten con la aceptación y apoyo de todos los niveles jerárquicos de cada una de las Entidades de la APE.

A continuación, se refiere una lista de las personas o dueños de procesos o administradores que se involucraron en la creación, revisión y aprobación de los documentos de políticas de seguridad de la Información para el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Unidad de Planeación y Control de TIC´s.
- Unidad de Automatización y Gobierno de TIC´s.
- Unidad de Red Estatal y Telecomunicaciones.
- Unidad de Innovación de Sistemas Financieros.
- Departamento de Infraestructura Tecnológica.
- Los técnicos y grupo de trabajo de soporte técnico de la *Dirección General de Tecnologías e Innovación Digital.*
- Los Administradores de las plataformas tecnológicas bajo el resguardo de la *Dirección General de Tecnologías e Innovación Digital.*
- Representantes de los grupos de usuarios afectados por las políticas o política específica de seguridad
- Administrador responsable del área
- Asesores legales.

Esta lista es representativa pero no necesariamente limitativa.

IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Las características para una buena implementación de las políticas de seguridad son:

Todas las políticas de seguridad de la información, registradas en este documento cumplen el precepto **"Debe ser posible",** toda vez que su implementación a través de los sistemas de procedimientos administrativos implementados por la *Dirección General de Tecnologías e Innovación Digital*, así como su publicación de las guías aceptables de uso o cualquier otro método apropiado cubren el procedimiento correspondiente.

Las Políticas de la *Dirección General de Tecnologías e Innovación Digital* cumplen el precepto **"Debe ser viable",** toda vez que no es forzado su cumplimiento. Mediante herramientas de control y donde sea necesario, el Oficial de Seguridad de la Información de la *Dirección General de Tecnologías e Innovación Digital*, verifica su cumplimiento y en su caso diseña el empleo de sanciones donde la prevención no pueda ser técnicamente posible.

Las Políticas de Seguridad de la información de la *Dirección General de Tecnologías e Innovación Digital* cumplen el precepto "**Debe definir claramente",** toda vez que las áreas de

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

responsabilidad de los usuarios, administradores y ejecutivos de la organización estén plenamente definidas.

Una vez que la política ha sido autorizada y establecida, debe comunicarse de forma clara y suficiente a los usuarios, grupo de trabajo y administradores.

Finalmente, cada política debe ser revisada de forma regular para verificar el éxito de su implantación y si cubre las necesidades de seguridad requeridas por la organización.

Etapas en el Desarrollo de las Políticas de Seguridad de la *Dirección General de Tecnologías e Innovación Digital***:**

Fase de desarrollo:	**Fase de implementación:**
Creación (1) Revisión (2) Aprobación (3)	Comunicación (4) Cumplimiento (5) Excepciones (6
Fase de mantenimiento:	**Fase de eliminación:**
Concienciación (7) Monitoreo (8) Garantía de Cumplimiento (9) Mantenimiento (10)	Retiro (11

En la elaboración de las políticas de Seguridad de la Información de la *Dirección General de Tecnologías e Innovación Digital* se cubrieron las 11 etapas que deben realizarse a través de "la vida" de una política. Estas 11 etapas pueden ser agrupadas en 4 fases:

1) **Fase de desarrollo**: durante esta fase la política es creada, revisada y aprobada.
2) **Fase de implementación**: en esta fase la política es comunicada y acatada (o no cumplida por alguna excepción).
3) **Fase de mantenimiento**: los usuarios deben ser conscientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).
4) **Fase de eliminación**: La política se retira cuando no se requiera más.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

1.- Creación: Planificación, investigación, documentación, y coordinación de la política

El primer paso en la fase de desarrollo de cada una de las políticas es la planificación, la investigación y la redacción de la política o, tomado todo junto. La creación de una política implica identificar por qué se necesita la política (por ejemplo, requerimientos legales, regulaciones técnicas, contractuales u operacionales); determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política, así como garantizar la factibilidad de su implementación. La creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas (es decir, que autoridades deben aprobarla, con quién se debe coordinar el desarrollo y estándares del formato de redacción), y la investigación de las mejores prácticas en la industria para su aplicabilidad a las necesidades organizacionales actuales. De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos y estándares de la *Dirección General de Tecnologías e Innovación Digital*, al igual que la coordinación con entidades internas y externas que la política afectará, para obtener información y su aceptación. En general, la creación de una política es la función más fácil de entender en el ciclo de vida de desarrollo de esta.

2.- Revisión: Evaluación independiente de la política

La revisión de la política es la segunda etapa en la fase de desarrollo del ciclo de vida. Una vez que la documentación de la política ha sido creada y la coordinación inicial ha comenzado, esta debe ser remitida a un grupo (o un individuo) independiente para su evaluación antes de su aprobación final. Hay varios beneficios de la revisión independiente: una política más viable a través de la observación de individuos que tienen una perspectiva diferente o más vasta que la persona que redactó la política; apoyo más amplio para la política a través de un incremento en el número de involucrados; aumento de credibilidad en la política gracias a la información recibida de diferentes especialistas del grupo de revisión. Propio de esta etapa es la presentación de la política a los revisores, ya sea de manera formal o informal, exponiendo cualquier punto que puede ser importante para la revisión, explicando su objetivo, el contexto y los beneficios potenciales de la política y justificando por qué es necesaria. Como parte de esta función, se espera que el creador de la política recopile los comentarios y las recomendaciones para realizar cambios en la política y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de la política lista para la aprobación por las directivas.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.- Aprobación: Obtener la aprobación de la política por parte de las directivas

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo de la administración de la *Dirección General de Tecnologías e Innovación Digital,* mediante la firma de la persona con mayor posición de autoridad o jerarquía.

La aprobación permite iniciar la implementación de la política. Requiere que el proponente de la política haga una selección adecuada de la autoridad de aprobación, que coordine con dicho funcionario, presente las recomendaciones emitidas durante la etapa de revisión y una vez que la política ha sido aprobada formalmente, continuar con la fase de implementación. La comunicación de la política es la primera etapa que se realiza en esta fase. La política debe ser inicialmente difundida a los miembros de las Dependencias y Entidades del Estado, organización o a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de cierto servicio, etc.). Esta etapa implica determinar el alcance y el método inicial de distribución de la política (es posible que deban tenerse en cuenta factores como la ubicación geográfica, el idioma, la cultura y línea de mando que será utilizada para comunicar la política). Debe planificarse esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

4.- Comunicación: garantizar que se conozca

Mediante reuniones informativas, cursos de entrenamiento, mensajes de correo, notas informativas, etcétera; y desarrollo y difusión de material de concienciación (presentaciones, láminas de publicidad, circulares, trípticos, etc., se debe garantizar que sean de conocimiento de todo el personal.

5.- Cumplimiento: Implementar la política

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Implica trabajar con otras personas de las Dependencias y Entidades de la APE, directores, subdirectores, jefes de departamento y los jefes de dependencias (de división o de sección) para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y oficinas; asegurando que la política es entendida por aquellos que requieren implementarla, monitorearla, darle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas. Dentro de estas actividades está la elaboración de informes a la administración, del estado que guarda la implementación de la política.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.- Excepciones: Gestionar las situaciones donde la implementación no es posible

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se planeó al inicio. Por esto, cuando los casos lo ameriten, es probable que se requieran excepciones a la política para permitir a ciertas oficinas o personas el no cumplimiento de la política. Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción. El proceso también debe permitir excepciones permanentes a la política al igual que la no aplicación temporal por circunstancias de corta duración.

7.- Concienciación: Garantizar que se genere la conciencia de la política de manera continua

La etapa de concienciación de la fase de mantenimiento comprende los esfuerzos continuos realizados para garantizar que las personas están conscientes de la política y buscan facilitar su cumplimiento. Esto es hecho al definir las necesidades de concienciación de los diversos grupos de audiencia dentro de la organización (directivos, jefes de dependencias, usuarios, etc.); en relación con la adherencia a la política, determinar los métodos de concienciación más efectivos para cada grupo de audiencia. La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento. La tarea final es medir la concienciación de personal de la APE con la política y ajustar los esfuerzos de acuerdo con los resultados de las actividades medidas.

8.- Monitoreo: se debe supervisar que se cumplan

Durante la fase de mantenimiento, la etapa de monitoreo es realizada para seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política. Esta información se obtiene de la observación del personal, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a los incidentes. Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la política, a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

9.- Garantía de cumplimiento: Afrontar las contravenciones de la política

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Esto significa que una vez que la contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (revisión del proceso y mejoramiento), la tecnología (actualización) y a las personas (acción disciplinaria) involucradas en la contravención, con el fin de reducir la probabilidad de que vuelva a ocurrir. Se recomienda incluir información sobre las acciones correctivas adelantadas, para garantizar el cumplimiento en la etapa de concienciación.

10.- Mantenimiento: Asegurar que la política esté actualizada

La etapa de mantenimiento está relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios (en la tecnología, los procesos, las personas, la organización, el enfoque del negocio, etc.) que puede afectar la política; recomendando y coordinando modificaciones, resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio. Esta etapa también garantiza la disponibilidad continuada de la política para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se requieran cambios a la política, las etapas realizadas antes deben ser verificadas, en particular las etapas de revisión, aprobación, comunicación y garantía de cumplimiento.

11.- Retiro: Prescindir de la política cuando no se necesite más

Después que la política ha cumplido con su finalidad y no sea necesaria (por ejemplo, la empresa cambió la tecnología a la cual aplicaba o se creó una nueva política que la remplazó) entonces debe ser retirada. La etapa de retiro corresponde a la fase de eliminación del ciclo de vida de la política y es la etapa final del ciclo. Esta función implica retirar una política que sea inútil o innecesaria del inventario de políticas activas, para evitar confusión, archivarla para futuras referencias y documentar la información sobre la decisión de retirarla (es decir, la justificación, quién autorizó, la fecha, etc.).

Estas cuatro fases del ciclo de vida reúnen 11 etapas diferentes que deben seguirse durante el ciclo de vida de una política específica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

PRÁCTICAS UTILIZADAS PARA LA REDACCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA *DIRECCIÓN GENERAL DE TECNOLOGÍAS E INNOVACIÓN DIGITAL*

En todos los casos las políticas incluyen los siguientes 12 tópicos:

1	La declaración de la política (cuál es la posición de *Dirección General de Tecnologías e Innovación Digital* describiendo lo que se desea regular).
2	Nombre y cargo de quien autoriza o aprueba la política en este caso el Jefe de Unidad o Departamento.
3	El grupo o la persona que es el autor o el proponente de la Política, en este caso el Oficial de Seguridad de la Información apoyado por su Unidad de Riesgos.
4	Debe especificarse quién debe acatar la política (es decir, a quién está dirigida) y quién es el responsable de garantizar su cumplimiento.
5	Indicadores para saber si se cumple o no la política.
6	Referencias a otras políticas y regulaciones en las cuales se soporta o con las cuales tiene relación dentro de la *Dirección General de Tecnologías e Innovación Digital* o de la Dirección de Servicios Tecnológicos.
7	Enunciar el proceso para solicitar excepciones.
8	Describir los pasos para solicitar cambios o actualizaciones a la política.
9	Explicar qué acciones se seguirán en caso de contravenir la política.
10	Fecha a partir de la cual tiene vigencia la política.
11	Fecha cuando se revisará la utilidad y la obsolescencia de la política.
12	Incluir la dirección de correo electrónico, página web y el teléfono de la persona o personas que se pueden contactar en caso de preguntas o sugerencias.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

DEFINICIÓN DE RESPONSABILIDADES EN EL DESARROLLO DE POLÍTICAS

La Jefatura de Unidad de Planeación y Control de TICs, en coordinación con las demás Jefaturas de Unidad de la DGTID, son los encargados de formular y diseñar la gran mayoría de las etapas en el ciclo de creación de cada una de las políticas, figurando también como el proponente para el diseño y redacción de las políticas relacionadas con la protección de los activos de información de la *Dirección General de Tecnologías e Innovación Digital*, sin embargo, por procedimiento estándar de la Dirección de Servicios Tecnológicos, las políticas son revisadas por cada dueño del proceso y operación, a efecto de que estas no se conceptualicen con un control centralizado, con este procedimiento se obtiene el control de:

Separación de tareas. El principio de separación de tareas es aplicado para determinar la responsabilidad de una etapa en particular para garantizar que las revisiones y ajustes necesarios sean aplicados. Para proveer una perspectiva más amplia y diferente, un directivo, o un grupo que sea independiente a la Unidad de Riesgos, debe revisar la política y una directiva superior al proponente, debe encargarse de aprobar la política. Para disminuir los posibles conflictos de intereses, grupos u organizaciones de auditoría externas pueden ser invitados a realizar una evaluación independiente del cumplimiento de las políticas para ser consistentes con el principio de separación de tareas.

Eficiencia. Adicionalmente, por razones de eficiencia, las Jefaturas Unidad y de Departamento de la *Dirección General de Tecnologías e Innovación Digital*, tienen responsabilidad para la realización de ciertas etapas del ciclo de vida del desarrollo de una política.

Alcance del control. Los límites en el alcance del control que la Unidad de Riesgos que propone en esta política, sólo puede jugar un papel limitado en el monitoreo y en la garantía del cumplimiento de esta debido a que la Unidad de Riesgos no puede estar en todos los sitios, en todo momento, donde ésta debe ser implementada.

Autoridad. Límites en la autoridad que se ejerce.

Conocimiento. De acuerdo con el alcance de la política, la labor de evaluación es realizada por el Oficial de Seguridad de la Información.

Aplicabilidad. ¿Qué unidades de operación de la *Dirección General de Tecnologías e Innovación Digital* son afectadas por la política? ¿La política aplica a uno o varios procesos?, ¿Sólo a los usuarios de cierta plataforma en particular o a todo la APE?

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

RESPONSABILIDADES EN EL MODELO DE CICLO DE VIDA DE LA POLÍTICA

Para garantizar que todas las etapas del ciclo de vida sean realizadas de manera apropiada y las responsabilidades para su ejecución sean asignadas adecuadamente, la *Dirección General de Tecnologías e Innovación Digital* debe establecer un marco de referencia para facilitar el entendimiento, promover la aplicación consistente, establecer una estructura jerárquica para soportar mutuamente los distintos niveles de políticas y acomodar efectivamente los frecuentes cambios tecnológicos y organizacionales.

CRITERIO PARA EL DESARROLLO DE LAS PRESENTES POLÍTICAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA TECNOLÓGICA DE LA DIRECCIÓN GENERAL DE TECNOLOGIAS E INNOVACIÓN.

Las presentes políticas de seguridad de la información se han realizado de acuerdo con los lineamientos establecidos en la Norma ISO/IEC 27001:2005, primera edición para el Sistema de Gestión de la Seguridad de la Información.

Cada segmento de políticas de seguridad está asociado a la nomenclatura establecida en la norma referida con el objeto de hacer más fácil la localización y referencia de cada política de seguridad.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

GLOSARIO DE TÉRMINOS PARA LA ELABORACIÓN DE POLÍTICAS DE SEGURIDAD

RFC 2119: Para la elaboración del MPSI (Manual de Políticas de Seguridad de la Información) se tomó como referencia el documento que proporciona palabras clave a utilizar, para indicar niveles de requerimiento del cual se refieren a continuación la lista de palabras para la ejecución de acciones definidas en las políticas de seguridad de la *Dirección General de Tecnologías e Innovación Digital*.

Las palabras clave "DEBE", "NO DEBE", "REQUERIDO", "DEBIERA", "NO DEBIERA", "DEBERÍA", "NO DEBERÍA", "RECOMENDADO", "PODRÍA" y "OPCIONAL" deben ser interpretados de acuerdo con los criterios establecidos en este documento.

DEBE. Esta palabra o los términos "REQUERIDO" o "DEBIERA" significan que la definición es requerida totalmente por la especificación y con carácter obligatorio.

"NO DEBE". Esta frase o la de "NO DEBIERA" significan que la definición es una prohibición absoluta de la especificación.

"DEBERÍA", Esta palabra o el adjetivo "RECOMENDADO" significan que podrían existir razones válidas en una circunstancia particular para ignorar el hecho, pero que las implicaciones totales deben ser comprendidas y analizadas cuidadosamente antes de elegir un curso diferente de eventos o acciones.

"NO DEBERÍA". Esta frase o la de "NO RECOMENDADO" significan que podrían existir razones válidas en circunstancias particulares cuando un evento específico es aceptable o incluso útil, pero que las implicaciones deben ser totalmente comprendidas y cuidadosamente analizadas antes de implementar cualquier acción descrita en la especificación.

"PODRÍA". Esta palabra o el adjetivo "OPCIONAL" significan que un evento o elemento es totalmente opcional dentro de una especificación.

Guía en el uso de este documento de frases y palabras clave. - Los imperativos definidos en este documento deben ser empleados con cuidado y previo análisis. En particular la palabra "DEBE", únicamente debe ser usada donde sea requerida para especificar o para limitar el daño potencial de una acción o inacción.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Consideraciones de seguridad. Estos términos son frecuentemente empleados para especificaciones de seguridad y dentro de los ámbitos de estas actividades. Los efectos de seguridad de la NO implementación de un "DEBE" o "DEBERÍA", o de ejecutar algunas acciones donde la especificación dice "NO DEBE" o "NO DEBERÍA" pueden parecer simples o problema de sintaxis. Estas aparentes diferencias deben ser claramente especificadas para evitar o limitar los daños a la información o a los medios de información.

CRITERIO PARA EL DESARROLLO DE POLÍTICAS DE SEGURIDAD

Referencia ISO 27001:2005. A 5 Políticas de Seguridad. A 5.1 Directrices de la Dirección General de Tecnologías e Innovación Digital en seguridad de la información.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión, concluido***
A 5.1 A 5.1.2	*Directrices de la Dirección General de Tecnologías e Innovación Digital.* Revisión de las políticas para la seguridad de la información.	2	2.0	Concluido
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Definición del criterio para el desarrollo de las políticas de seguridad de la información para el uso y aprovechamiento de Tecnologías de la Información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Objetivo

Establecer el criterio básico para la elaboración de políticas de seguridad para las Dependencias y Entidades del Estado, así como para los procesos, normas, métodos, técnicas, configuraciones y tecnologías y/o información de la DGTID

1.0 Propósito

Definir la filosofía única y principal para el desarrollo y especificación de las políticas, reglas, métodos, configuraciones y técnicas de seguridad de la información para La Administración Pública del Estado. Esta filosofía debe aplicar como criterio para todas las acciones presentes y futuras en materia de seguridad de la información.

2.0 Ámbito de Aplicación

Este criterio aplica para todos y cada uno de los objetos, procesos o procedimientos administrativos y de seguridad de la información tales como servicios, aplicaciones, accesos físicos y lógicos, protocolos, puertos, dispositivos, interfaces, equipos de comunicaciones y redes, sistemas operativos, programas, sistemas instalados o por instalar dentro de las instalaciones o zonas de responsabilidad de la *Dirección General de Tecnologías e Innovación Digital*, así como al uso de tecnología presente o futura.

3.0 Política

3.1 Descripción de Política

Todo lo que no esté explícitamente permitido está prohibido

Se deben especificar por escrito en las políticas, todos y cada uno de los servicios de información que sean permitidos en para las Dependencias y Entidades del Estado. Cualquier otro medio de información física o lógica que no se encuentre explícitamente permitida debe estar prohibido mediante técnicas, procedimientos, métodos, programas, sistemas, software, configuraciones o cualquier medio posible y disponible por para las Dependencias y Entidades del Estado.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe/a de la Unidad de Planeación y Control de TIC´S

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Administración y ejecución:	Personal de TI y de la Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente a la Administración Pública del Estado, usuarios y proveedores.

El personal de la Dirección de Servicios Tecnológicos debe ser responsable de la administración de las normas de seguridad de la *Dirección General de Tecnologías e Innovación Digital*, así como de la aplicación de los criterios de esta política para la instalación y configuración de los servicios, aplicaciones, accesos, protocolos, programas y sistemas requeridos por para las Dependencias y Entidades del Estado.

3.3 Monitoreo

Se deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la configuración de todos y cada uno de los equipos informáticos de la Dirección General de Tecnologías e Innovación Digital tales como: ruteadores, switches, concentradores, sistemas operativos, servicios, aplicaciones, bases de datos, programas y sistemas (propiedad y en operación por parte de la Dirección General de Tecnologías e Innovación Digital), así como a los métodos de registro y control de acceso a las instalaciones de los centros de dato resguardados por las áreas responsables de las Dependencias y Entidades del Estado.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

4.0 Sanciones y Observaciones

Cualquier empleado que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Dirección Administrativa de la Secretaría de Finanzas del Poder Ejecutivo del Estado de Oaxaca, en base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo del Que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Personal responsable	Es la o las personas pertenecientes a la estructura orgánica de las Instituciones de la APE a cargo de infraestructura Tecnológica, designadas para realizar actividades específicas tales como administración de sistemas, administración de seguridad o administración de bases de datos.
Servicio	Es el sistema, programa o software que proporciona información como: correo electrónico, nombre de dominio, portales y páginas https, ftp, proxy y cualquier medio de software que permita el proceso, envío, recepción o redirección de información.
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Integridad	La información no debe ser alterada de tal forma que quede incompleta o incorrecta. A los usuarios no autorizados se les deben restringir los permisos para modificar o destruir información sensible.
Disponibilidad	La información debe ser accesible para usuarios autorizados en cualquier momento en que se necesite. La disponibilidad es una garantía de que la información pueda obtenerse en tiempo y frecuencia aceptable.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López Director *General* *Dirección General de Tecnologías e Innovación Digital*	Ing. Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: M.T.I. Ana Laura Ortega Aguilar Jefa de la Unidad de Planeación y Control de TIC´s Dirección de Servicios Tecnológicos - DGTID	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

AUTORIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Referencia ISO 27001:2005. A 5 Políticas de Seguridad. A 5.1 Directrices de la Dirección General de Tecnologías e Innovación Digital en seguridad de la información.

Control	***Área de aplicación***	***Actualización***	***Versión***	***Estado actual del procedimiento: Programado, en proceso, en revisión concluido***
A 5.1 A 5.1.2	*Directrices de la Dirección General de Tecnologías e Innovación Digital en seguridad de la información.* Revisión de las políticas para la seguridad de la información.	2	2.0	Concluido
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Autorización de políticas de seguridad.

Objetivo

La publicación y aplicación de las políticas de seguridad de la información del uso y aprovechamiento de Tecnologías de la Información, así como cualquier modificación o actualización de estas deben ser autorizadas exclusivamente por la Dirección General de Tecnologías e Innovación Digital.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

1.0 Propósito

Que las políticas de seguridad de la información para el uso y aprovechamiento de Tecnologías de la Información y las Comunicaciones, se mantengan a lo largo del tiempo de forma homogénea y coherente, que sean conocidas y comprendidas por los usuarios y grupos de interés. Únicamente pueden ser autorizadas por el Director General de Tecnologías e Innovación Digital, y/o la Dirección de Servicios Tecnológicos. Para su aplicación y estricto cumplimiento, el personal de las Dependencias y Entidades del Estado, usuarios y proveedores del uso y aprovechamiento de Tecnologías de la Información deberán ser informados y en su caso capacitados.

2.0 Ámbito de Aplicación

Las políticas de Seguridad de la Información para el uso y aprovechamiento de Tecnologías de la Información y las Comunicaciones aplicarán a todos los usuarios, el personal, y grupos interesados que hagan uso de equipos, dispositivos, programas, aplicaciones, sistemas y cualquier medio de información, así como a procesos, procedimientos y reglas relacionadas con la estructura orgánica de la APE y que en lo general hagan uso y aprovechamiento de Tecnologías de la Información, o bajo su ámbito de responsabilidad, tales como usuarios y/o proveedores de las Dependencias y Entidades del Estado.

3.0 Política

3.1 Descripción de Política

Cualquier solicitud de instalación o implementación de servicios, programas, sistemas, protocolos, accesos, aplicaciones, equipo o dispositivos, deben ser analizadas por la Jefatura de Unidad de Planeación y Control de TICs, de la *Dirección General de Tecnologías e Innovación Digital* con el objeto de determinar el impacto, beneficios y riesgos probables de estas acciones.

La instalación y/o configuración de los elementos solicitados deben cumplir estrictamente los términos definidos en la política: “Criterio para el Desarrollo de las Políticas de Seguridad”, establecida en el primer capítulo “Política de Seguridad” de este manual, y debe ser realizada por el personal de la Jefatura de Unidad de Planeación y Control de TICs, especializado o por el personal autorizado por la Dirección de Servicios Tecnológicos para tal efecto.

Los cambios y/o actualizaciones a las políticas de seguridad de la información para el uso y aprovechamiento de Tecnologías de la Información, deben ser documentados, justificados y autorizados por parte de la Dirección de Servicios Tecnológicos.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

El estricto cumplimiento de las políticas de seguridad de la información aplica para todo usuario, administradores y grupos de interés que hagan uso y aprovechamiento de Tecnologías de la Información propiedad del Estado, así como para proveedores sin excepción.

La publicación de las políticas de seguridad debe realizarse a través del portal web de la Dirección General de Tecnologías e Innovación Digital, para el conocimiento y cumplimiento de todo el personal administrativo de la APE, usuarios, administradores de TI, Grupos de Interés, y proveedores del Estado de Oaxaca.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios, y proveedores.

Las autorizaciones correspondientes a los cambios y actualizaciones a las mismas serán bajo expresa autorización por la *Dirección General de Tecnologías e Innovación Digital*, previo dictamen de impacto y riesgos, presentado por la Dirección de Servicios Tecnológicos. Cada modificación o solicitud de modificación a las políticas de seguridad de la información deberán contar con el aval de la Dirección de Servicios Tecnológicos.

La responsabilidad de la supervisión y cumplimiento de las políticas de seguridad se realizará por parte de la Jefatura de la Unidad de Planeación y Control de TICs de la Dirección de Servicios Tecnológicos – DGTID.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TICs, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.4 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal de la Jefatura de la Unidad de Planeación y Control de TIC's; al menos una vez al año.

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información que tiene bajo administración y custodia la DGTID.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Informe Detallado de Riesgos.	Es el documento donde se especifican tanto el impacto en términos de recursos y viabilidad, así como de los riesgos en términos de vulnerabilidades detectadas o potenciales de un servicio, programa, software, sistema operativo o cualquier medio de información físico o lógico.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: Diciembre 2020

Autoriza	Revisa
Eduardo José Herrerías López Director *General de Tecnologías e Innovación Digital.*	Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: Ana Laura Ortega Aguilar Jefa de la Unidad de Planeación y Control de TIC´s Dirección de Servicios Tecnológicos - DGTID.	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

ORGANIZACIÓN INTERNA

FACULTADES DE LA DIRECCIÓN GENERAL DE TECNOLOGÍAS E INNOVACIÓN DIGITAL PARA LA PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA TECNOLÓGICA DEL GOBIERNO DEL ESTADO DE OAXACA.

Referencia ISO 27001:2005. A 6 Aspectos Organizativos de la Seguridad de la Información. A.6.1. Organización Interna.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión concluido***
A. 6.1 A.6.1.1 A.6.1.2	Organización Interna Asignación de responsabilidades para la seguridad. de la información Segregación de tareas.	2	2.0	Concluida
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Facultades de la Dirección General de Tecnologías e Innovación Digital para la preservación de la seguridad de los sistemas de información e infraestructura tecnológica para el uso y aprovechamiento de Tecnologías de la Información y las Comunicaciones en el Estado de Oaxaca.

Objetivo

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Definir los alcances de las facultades del personal adscrito a la Dirección General de Tecnologías e Innovación Digital para preservar y mantener la seguridad de los sistemas de información y plataforma tecnológica patrimonio del Estado de Oaxaca.

1.0 Propósito

Establecer los alcances y facultades de la Dirección General de Tecnologías e Innovación Digital para proteger y salvaguardar los sistemas de información e infraestructura tecnológica patrimonio del Estado de Oaxaca, sobre el uso y aprovechamiento de Tecnologías de la Información, tomando en cuenta en todo momento las características de la seguridad que son: ***Integridad, Disponibilidad y Confidencialidad.***

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para todo el personal asignado a la Dirección General de Tecnologías e Innovación Digital. Sin embargo, el alcance de las acciones necesarias para salvaguardar los sistemas de información y la infraestructura tecnológica determinadas podrá ser a todos los servidores públicos de las Dependencias de la APE y sobre los sistemas y plataformas tecnológicas que tenga en administración o custodia la DGTID, inclusive en términos geográficos, físicos o lógicos.

3.0 Política

3.1 Descripción de Política

El personal de la *Dirección General de Tecnologías e Innovación Digital* está facultado para realizar cualquier acción necesaria que contribuya a salvaguardar los sistemas de información y la infraestructura tecnológica de las Dependencias y Entidades del Estado en cualquiera de sus complejos tecnológicos e instalaciones, sin perjuicio de su relación laboral por las acciones necesarias que se ejecuten para protección de la seguridad de los sistemas de información e infraestructura tecnológica.

Estas facultades pueden ir desde la emisión de recomendaciones a las áreas o personal adscrito en las Dependencias y Entidades del Estado con el objeto de preservar y privilegiar la seguridad de los sistemas de información, hasta la cancelación de los accesos a los sistemas de información, el acceso a Internet y/o los servicios de telefonía y/o telecomunicaciones en caso de infecciones, ataques o intrusiones no autorizadas que no puedan contenerse o controlarse, los cuales incluirán pero no limitarán a:

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Envío, transmisión, transferencia, copia, impresión y/o extracción de información clasificada.
- Intrusión no autorizada por cualquier medio físico o lógico a los sistemas de información y/o infraestructura tecnológica.
- Incidentes de seguridad física a las instalaciones de la APE.
- Incidentes de seguridad lógica.
- Ataques en progreso a los sistemas de información y/o infraestructura tecnológica.
- Ataques y/o infecciones por virus informáticos
- Violaciones a las presentes políticas de seguridad de los sistemas de información, a las normas, reglamentos o leyes en la materia que comprometan las características de la seguridad de la información como son: confidencialidad, integridad y disponibilidad.
- A cualquier otro acto que comprometa la seguridad, los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

Las acciones de contención deberán estar avaladas por la Dirección de Servicios Tecnológicos. Sin embargo, para los casos específicos de interrupción de servicios de información derivados de incidentes en seguridad, la Jefatura de la Unidad de Planeación y Control de TIC´s, deberá proporcionar el análisis forense del incidente que justifique plenamente, la interrupción de servicios.

La Dirección *General de Tecnologías e Innovación Digital* a través de la Dirección de Servicios Tecnológicos y la Jefatura de la Unidad de Planeación y Control de TICs, es responsable de establecer y mantener las políticas, normas, lineamientos y procedimientos relativos a la seguridad de la información de la *Dirección General de Tecnologías e Innovación Digital*.

La *Dirección General de Tecnologías e Innovación Digital*, mediante los controles establecidos deberá garantizar que la información patrimonio del Estado está protegida con procesos que mantienen la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas e infraestructura que los soporta.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal administrativo, usuarios y grupos de interés perteneciente la Administración Pública del Estado, incluyendo terceros proveedores.

El personal de la *Dirección General de Tecnologías e Innovación Digital* debe ser responsable de la administración de la presente política de seguridad, así como de la aplicación de los criterios de esta política para preservar los sistemas de información y la infraestructura tecnológica que son patrimonio del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC´s deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, de reglamentos, jurídicos, financieros o de cualquier otra índole incluyendo los avances tecnológicos que tengan impacto en las facultades de la *Dirección General de Tecnologías e Innovación Digital*.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado de la Jefatura de la Unidad de Planeación y Control de TIC´s; por lo menos, una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Los servicios de auditoría al Sistema de Gestión de la Seguridad de la Información (SGSI), o a cualquier otro elemento de gestión de tecnología deberá ser efectuado por entidades externas a para las Dependencias y Entidades del Estado por lo menos una vez al año.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Facultades	Conjunto de acciones permitidas al personal de la *Dirección General de Tecnologías e Innovación Digital*, sin perjuicio de su relación laboral con para las Dependencias y Entidades del Estado.
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Integridad	La información no debe ser alterada de tal forma que quede incompleta o incorrecta. A los usuarios no autorizados se les deben restringir los permisos para modificar o destruir información sensible.
Disponibilidad	La información debe ser accesible para usuarios autorizados en cualquier momento en que se necesite. La disponibilidad es una garantía de que la información pueda obtenerse en tiempo y frecuencia aceptable.
Sistemas de información	Software, aplicaciones, programas, rutinas, código o algoritmos necesarios para el almacenamiento, procesamiento o recuperación de información.
Infraestructura tecnológica	Conjunto de elementos de hardware o software necesario para el almacenamiento, procesamiento, recuperación o transmisión de datos e información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
Eduardo José Herrerías López Director *General de Tecnologías e Innovación Digital.*	Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: Ana Laura Ortega Aguilar Jefa de la Unidad de Planeación y Control de TIC´s Dirección de Servicios Tecnológicos - DGTID.	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

ACUERDOS DE CONFIDENCIALIDAD

Referencia ISO 27001:2005. A.6 Aspectos Organizativos de la Seguridad de la Información. A.6.1. Organización Interna

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.6.1 A.6.1.5	Organización Interna Acuerdos de confidencialidad	2	2.0	Concluida
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Acuerdos de confidencialidad establecidos con los usuarios, proveedores y terceros que presten sus servicios a la Administración Pública del Estado de Oaxaca.

Objetivo

Establecer acuerdos de confidencialidad en los contratos que se llevan a cabo terceros y proveedores que presten sus servicios dentro de la Administración Pública del Estado, con la finalidad de establecer un control que evite que datos o cualquier información, sea divulgada sin las autorización y pleno conocimiento del Estado de Oaxaca.

1.0 Propósito

Evitar que la información confidencial y patrimonio de la APE, sea divulgada o compartida.

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para todo el personal de la *Dirección General de Tecnologías e Innovación Digital* que sea contratado por cualquiera de

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

las modalidades, proveedores y terceros que presten sus servicios a través de La DGTID a la Administración Pública del Estado de Oaxaca.

3.0 Política

3.1 Descripción de Política

Como parte de los términos y condiciones iníciales de empleo, el personal de la *Dirección General de Tecnologías e Innovación Digital*, proveedores y terceros que presten sus servicios a la Administración Pública del Estado de Oaxaca, firmarán un "Acuerdo de Confidencialidad" o no divulgación, en lo que respecta al tratamiento de la información que por medio de los sistemas tenga bajo operación, administración y custodia la *Dirección General de Tecnologías e Innovación Digital*. El original firmado de dicho acuerdo deberá permanecer en resguardo en los archivos en tránsito de la *Dirección General de Tecnologías e Innovación Digital*.

Asimismo, mediante la firma de dicho acuerdo, el personal de la *Dirección General de Tecnologías e Innovación Digital*, proveedores y terceros que presten sus servicios a la Administración Pública del Estado de Oaxaca, declararán conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deberán ser especificadas a fin de no violar el derecho a la privacidad del personal mencionado.

Los Proveedores y terceros adjunto o como parte de su relación contractual establecerán la responsabilidad de su personal en materia de seguridad de la información mediante el acuerdo de confidencialidad. Dichas condiciones establecen que son totalmente responsables de su personal y, por lo tanto, deberán asumir las responsabilidades que correspondan.

Los derechos y obligaciones del personal de la *Dirección General de Tecnologías e Innovación Digital*, proveedores y terceros que prestan sus servicios a la Administración Pública del Estado de Oaxaca, relativos a este acuerdo de confidencialidad, prevalecerán a favor del Estado, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de su respectivo contrato.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID.
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos.
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos.
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y grupos de interés proveedores.

La *Dirección General de Tecnologías e Innovación Digital*, deberá ser responsable de la verificación de la presente política de "Acuerdo de Confidencialidad", así como de la aplicación de esta, para evitar riesgos en cuanto a la divulgación de la información.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC´s, deberá realizar una revisión periódica de los "Acuerdos de Confidencialidad" y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, de reglamentos (jurídicos, financieros o de cualquier otra índole).

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por el uso y aprovechamiento de Tecnologías de la Información o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información,

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Proveedores Terceros	Personal de proveedores, contratistas, consultores y becarios que no son empleados de la DGTID, pero que prestan algún servicio técnico o profesional al APE.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Autoriza	Revisa
Eduardo José Herrerías López Director *General de Tecnologías e Innovación Digital.*	Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: Ana Laura Ortega Aguilar Jefa de la Unidad de Planeación y Control de TIC´s Dirección de Servicios Tecnológicos - DGTID.	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

IDENTIFICACIÓN DE LOS RIESGOS DERIVADOS DEL ACCESO DE TERCEROS

Referencia ISO 27001:2005. A.6 Aspectos Organizativos de la Seguridad de la Información. A.6.2 Terceros.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.6.2 *A.6.2.1*	Terceros Identificación de los riesgos derivados del acceso de terceros	2	2.0	Concluida
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Identificación de los riesgos derivados del acceso de terceros con quien tiene relación de trabajo la DGTID.

Objetivo

Identificar los riesgos para dispositivos de procesamiento de información, derivados de los procesos de negocio que la DGTID requiera realizar con terceros, así como implantar los controles apropiados antes de otorgar el acceso.

1.0 Propósito

Establecer los controles necesarios para el manejo y protección de la información y de los dispositivos de procesamiento que por motivos de su relación contractual sean intervenidos por terceros en función de la prestación de servicios a través de la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para todos los proveedores y terceros que presten sus servicios a la Administración Pública del Estado por medio de la DGTID.

3.0 Política

3.1 Descripción de Política

Cuando exista la necesidad de otorgar acceso a terceras partes, la DGTID como custodio de los sistemas de información del Estado, llevará a cabo y documentará una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en consideración:

- Tipo de acceso requerido (físico y/o lógico y a que recurso)
- Motivos para los cuales se solicita el acceso
- El valor de la información a la que tendrá acceso

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la *Dirección General de Tecnologías e Innovación Digital* establecerán los controles, requerimientos de seguridad y acuerdos de confidencialidad aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar.

En ningún caso se deberá otorgar el acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta que se hayan implementado los controles apropiados, y se haya firmado un contrato y acuerdo de confidencialidad, que definan las condiciones para el acceso o la conexión. En todos los casos el requirente de acceso deberá justificar su necesidad de acceso o conexión, en el entendido que la observación y contemplación no son suficientes para acceder sobre todo a los centros de procesamiento.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

La *Dirección General de Tecnologías e Innovación Digital*, debe ser responsable de la verificación de la presente política de "acuerdo de confidencialidad", así como de la aplicación de esta, para evitar riesgos en cuanto a la divulgación de la información, el acceso a áreas restringidas o sensibles que pongan en riesgo las condiciones de seguridad de la infraestructura.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos, deberá realizar una revisión periódica de la vigencia de los "acuerdos de confidencialidad" y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, de reglamentos (jurídicos, financieros o de cualquier otra índole).

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal que autorice la Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos, por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

5.0 Definición de Términos

Término	***Definición***
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Proveedores o Terceros	Proveedores, contratistas, consultores, becarios o auditores externos que no son empleados del Estado de Oaxaca, pero que prestan algún servicio técnico o profesional a la DGTID.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
Eduardo José Herrerías López Director *General de Tecnologías e Innovación Digital.*	Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: Ana Laura Ortega Aguilar Jefa de la Unidad de Planeación y Control de TIC´s Dirección de Servicios Tecnológicos - DGTID.	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

TRATAMIENTO DE LA SEGURIDAD EN CONTRATOS CON TERCEROS

Referencia ISO 27001:2005. A.6 Aspectos Organizativos de la Seguridad de la Información. A.6.2 Terceros.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.6.2 A.6.2.3	Terceros Tratamiento de la seguridad en contratos con Terceros	2	2.0	Concluida
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Tratamiento de la seguridad en contratos con terceros.

Objetivo

Determinar los requisitos respecto a la seguridad de los activos e información, que deberán contener los contratos que efectúe la DGTID con terceros respecto al acceso, procesamiento, comunicación o manejo de información o medios de procesamiento de información.

1.0 Propósito

Establecer los requerimientos y controles que aseguren que no existan malentendidos entre la DGTID y los terceros que presten sus servicios.

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para todo tercero como, proveedores consultores, contratistas o cualquiera que preste sus servicios la Administración Pública del Estado de Oaxaca por medio de la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.0 Política

3.1 Descripción de Política

La Jefatura de la Unidad de Planeación y Control de TICs de la Dirección de Servicios Tecnológicos, deberá revisar los contratos o acuerdos existentes que se efectúen con terceros, teniendo en consideración la aplicación de los siguientes controles y/o requerimientos:

- Clausula o acuerdo que les obligue al Cumplimiento de las Política de Seguridad de la *Información para el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, emitidas por la DGTID.*
- Clausula o acuerdo que les obligue a la Protección de los activos tecnológicos de la APE, incluyendo procedimientos para proteger los bienes patrimoniales del Estado, tanto físicos, como de la información, el software e infraestructura.
- Descripción de los servicios a otorgar.
- Nivel de servicio esperado y niveles de servicio aceptables.
- Permiso para la transferencia de personal cuando sea necesario.
- Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
- Existencia de Derechos de Propiedad Intelectual a favor del Estado.
- Definiciones relacionadas con la protección de datos.
- Acuerdos de control de accesos que contemplen:
    - Métodos de acceso permitidos, el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
    - Proceso de autorización de accesos y privilegios de usuarios.
    - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
- Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Proceso claro y detallado de administración de cambios.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Controles de protección física requeridos y los mecanismos que aseguren la implementación de estos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- Manejo de información y los activos al finalizar el contrato o acuerdo (o momento específico convenido durante la vigencia de este) para garantizar la recuperación o destrucción de la información.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

La Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos, es responsable de la verificación de la presente política de “Tratamiento de la seguridad en contratos con terceros”, así como de la aplicación de esta, para evitar riesgos en cuanto a la divulgación de la información y daño patrimonial en los activos de información e infraestructura tecnológica en custodia de la DGTID.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos, deberá realizar una revisión periódica de los controles aquí señalados, darle seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, de reglamentos (jurídicos, financieros o de cualquier otra índole).

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado por la Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos, por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Proveedores o Terceros	Personal, Proveedores, contratistas, consultores, Auditores, que no son empleados del Estado de Oaxaca, pero que prestan algún servicio técnico o profesional al APE.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

GESTIÓN DE ACTIVOS

RESPONSABILIDAD SOBRE LOS ACTIVOS

PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN

Referencia ISO 27001:2005. A.7 Gestión de Activos. A.7.1 Responsabilidad sobre los Activos.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión concluido***
A.7.1	Responsabilidad sobre los activos			
A.7.1.2	Propiedad de los activos	2	2.0	Concluido
Vigencia a partir de:		**marzo 2019**		

Título de la Política

Propiedad de la información en custodia de la DGTID.

Objetivo

Establecer los criterios de propiedad de la información en custodia de la DGTID.

1.0 Propósito

Definir los criterios de propiedad de la información con el objeto de definir cuando un conjunto de datos se considera propiedad absoluta y total por el uso y aprovechamiento de Tecnologías de la Información e incluye de forma especial, al conjunto de datos personales de los ciudadanos y se sujeta al cumplimiento de la Normativa Federal y Estatal vigente.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Este control aplica para todos los medios de información y datos de que disponga la DGTID y para los cuales se consideran medios impresos, digitales, sistemas de información, servicios de información, medios de almacenamiento electrónico/digital y cualquier otro medio que represente piezas parciales o elementos completos de información propiedad o patrimonio del Estado.

Igualmente, el ámbito de la aplicación contempla a todas y cada una de las áreas y personas que laboran bajo cualquier modalidad laboral para la DGTID, incluyendo usuarios, proveedores y terceros que de cualquier forma tengan acceso físico y/o lógico a datos e información perteneciente la Administración Pública del Estado y en custodia por la DGTID.

3.0 Política

3.1 Descripción de Política

Toda información y/o datos que se almacenen, procesen o consulten en medios o dispositivos físicos o lógicos por medios de los sistemas institucionales y que sea generada por motivos de las funciones y responsabilidades de los servidores públicos adscritos a la APE, es propiedad absoluta del Estado sin necesidad de reclamar su titularidad.

Toda información y/o datos que por medio de relaciones contractuales con terceros y que por esa razón hayan sido, adquiridos, pagados, arrendados, cedidos, donados, o por cualquier otro medio, es propiedad total del Gobierno del Estado de Oaxaca, y por lo tanto posee los derechos de uso y explotación de esta.

Toda información y/o datos que se encuentren en dispositivos de almacenamiento, procesamiento, de consulta, de comunicaciones, de transmisiones, o que atraviesen medios de comunicación que sean propiedad de las Instituciones o Dependencias de la APE, forman parte de los activos y patrimonio del Estado y, por lo tanto, no podrán ser sustraídos, almacenados transferidos por otros medios que no sean los Institucionales. Lo anterior aplica para casos específicos como son:

- Dispositivos de almacenamiento, procesamiento y/o consulta de información o datos.
- Dispositivos de comunicaciones de datos.
- Dispositivos de seguridad de la información y de protección de información.
- Medios portátiles de almacenamiento de información.
- Medios impresos.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Código de software, programas, rutinas, subrutinas, módulos, métodos, clases, algoritmos, funciones, procedimientos almacenados, disparadores, configuraciones o cualquier otra forma de código que forme parte de un software, sistema o servicio de información.

Se considera también propiedad del Estado, toda la información y datos creados, generados, actualizados y/o mantenidos por los servidores públicos de las Dependencias de la APE; por lo que estos no podrán ser almacenados o transmitidos por medios que no sean los institucionales. Lo anterior en total independencia de quien es el propietario de equipos, dispositivos, servidores, computadoras, impresoras, medios de comunicaciones, de transmisiones, sistemas de bases de datos, licenciamiento de hardware y/o software, configuraciones, cambios o cualquier otro medio o dispositivo donde se almacene, procese o consulte la información.

La *Dirección General de Tecnologías e Innovación Digital* deberá especificar claramente, por escrito, la asignación de las responsabilidades de la propiedad de la información para el acceso y manipulación de las bases de datos, los archivos maestros, aplicaciones o sistemas, debiendo asignar a las personas identidades electrónicas con los permisos necesarios para el desempeño de sus funciones, definiéndolos como propietarios una vez que los sistemas se hayan liberado y puesto en operación para los usuarios de la *Dirección General de Tecnologías e Innovación Digital*.

Con excepción de la información operacional relativa a la infraestructura tecnológica y la red de servicios, los administradores e integrantes de la *Dirección General de Tecnologías e Innovación Digital*, no deben ser propietarios de ninguna información perteneciente a otras áreas de negocio.

El alcance de operación de los integrantes de la *Dirección General de Tecnologías e Innovación Digital* es únicamente dentro del campo de operación que gestiona la Dirección de Servicios Tecnológicos, por lo que ninguno de sus integrantes podrá formar parte de grupos de trabajo con roles distintos a sus funciones.

Los custodios de la información son responsables de definir procedimientos de control específicos, administrar el control de acceso a la información y suministrar capacidades de recuperación, en concordancia con las instrucciones de los propietarios de la información.

Todos los activos de Tecnología de la Información (software y hardware), son activos exclusivamente para las operaciones de la *Dirección General de Tecnologías e Innovación Digital* y deben ser protegidos de acuerdo con su importancia y valor.

Todos los activos de Tecnología de la Información (aplicaciones, servidores, archivos, dispositivos de red, computadoras personales y portátiles, y cualquier otro medio de procesamiento y almacenamiento de información) propiedad del Estado deben tener un propietario o custodio (dueño). Dicho propietario es responsable de garantizar la integridad,

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

confidencialidad y disponibilidad de la información. Los propietarios de activos de información deben ser empleados permanentes de la *Dirección General de Tecnologías e Innovación Digital*.

Los empleados dueños de los activos deben aceptar por escrito la propiedad de sus activos describiendo conjuntamente sus responsabilidades sobre los activos como dueños. Los propietarios de activos pueden delegar algunas responsabilidades sobre sus activos a persona o entidad a quien se le reconoce como Custodio.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

El personal de la Dirección de Servicios Tecnológicos debe ser responsable de la administración de las normas de seguridad del uso y aprovechamiento de Tecnologías de la Información, así como de la aplicación de los criterios de esta política para la instalación y configuración de los servicios, aplicaciones, accesos, protocolos, programas y sistemas requeridos para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TICs, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la creación y/o mantenimiento de documentos, así como a la generación de reportes, consultas o pantallas generados por los sistemas de información, servicios de información, o dispositivos de tecnología de la información empleados por parte de la DGTID

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por la Jefatura de la Unidad de Planeación y Control de TICs al menos una vez al año.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.
Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Personal responsable	Es la o las personas pertenecientes a la plantilla de operación de la DGTID, designadas para realizar actividades específicas tales como administración de sistemas, administración de seguridad o administración de bases de datos.
Servicio	Es el sistema, programa o software que proporciona servicios de información como: correo electrónico, nombre de dominio, servicio de páginas https, ftp, proxy y cualquier medio de software que permita el proceso, envío, recepción o redirección de información.
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Integridad	La información no debe ser alterada de tal forma que quede incompleta o incorrecta. A los usuarios no autorizados se les deben restringir los permisos para modificar o destruir información sensible.
Disponibilidad	La información debe ser accesible para usuarios autorizados en cualquier momento en que se necesite. La disponibilidad es una

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

garantía de que la información pueda obtenerse en tiempo y frecuencia aceptable.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

USO ACEPTABLE DE LOS ACTIVOS

Referencia ISO 27001:2005. A.7 Gestión de Activos. A.7.1 Responsabilidad sobre los activos.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.7.1	Responsabilidad sobre los activos			
A.7.1.3	Uso Aceptable de los activos	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Política de uso aceptable de los recursos informáticos.

Objetivo

Definir los controles de seguridad de la información para el uso aceptable de la infraestructura tecnológica en administración y custodia de la DGTID.

1.0 Propósito

El propósito de esta política es definir los controles de seguridad de la información para el uso de los recursos informáticos y plataforma tecnológica en administración y custodia de la DGTID. Estas reglas están desarrolladas para proteger las características de información, así como el de promover el uso óptimo de estas tecnologías. El uso inapropiado expone a la APE, a riesgos de seguridad tales como: Ataques de virus, compromiso de la seguridad de los sistemas, redes de comunicaciones y servicios, así como, la pérdida de productividad y desviación de recursos.

2.0 Ámbito de Aplicación

Esta política aplica a todos y cada uno de los empleados, usuarios, contratistas, proveedores y externos, incluyendo al personal afiliado de terceros que prestan sus servicios para La Administración Pública del Estado. También aplica a todo el equipo, dispositivos y medios de información propiedad o en arrendamiento de la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.0 Política

3.1 Descripción de Política

- El uso aceptable de los recursos tecnológicos e infraestructura de la APE implica que los sistemas, servicios, medios de información y dispositivos deben ser empleados para actividades exclusivas relacionadas con los objetivos y responsabilidades de sus puestos de trabajo, así como para servir a los intereses de las Dependencias y Entidades del Estado exclusivamente en apego a la provisión de servicios.

- Los sistemas incluyen, pero no se limitan a los equipos de cómputo, software, sistemas operativos, medios de almacenamiento, cuentas de acceso a recursos de redes o correo electrónico, navegación en Internet, o servicios de impresión y fotocopiado, ftp o cualquier otro medio de almacenamiento, procesamiento, consulta o transmisión de información que sean propiedad del Estado.

- Cualquier uso inadecuado de los recursos o infraestructura tecnológica estará sujeta a medidas correctivas, apercibimiento o sanciones en total dependencia a su relación laboral con la Administración Pública del Estado de Oaxaca o del esquema de contratación para cada persona física o moral que lleve a cabo trabajos para el Estado.

Criterios de Uso y Propiedad

- Las mejores prácticas de administración para los recursos informáticos deben servir para proporcionar niveles aceptables de seguridad y privacidad de la información, por lo tanto, los usuarios deben cumplir con todas las precauciones necesarias ya que los datos que ellos crean en o a través de los sistemas institucionales de información, son propiedad y patrimonio del Estado.

- Los Servidores Públicos y personal contratado por la APE, son responsables de ejercer el mejor juicio posible para el uso racional de los recursos informáticos, así como el seguimiento puntual de esta política de seguridad.

- Los titulares de las unidades administrativas de la *Dirección General de Tecnologías e Innovación Digital* deben ser propietarios de las aplicaciones y equipo de cómputo que utilizan.

- Se sugiere que cualquier tipo de información que los usuarios consideren como sensible o vulnerable sea cifrada. Para conocer la guía para la clasificación de información, consulte

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

el *Estándar de Clasificación de Información* y la *Política de criterios de clasificación de información*.

- Con fines de seguridad y mantenimiento de las redes, equipo de cómputo y telecomunicaciones, las personas autorizadas por la DGTID, deberán realizar revisiones y/o monitoreo de los equipos de cómputo, sistemas y tráfico de las redes mediante los procesos de Mantenimiento y en horarios que no afecten la productividad de negocio.

- La DGTID, se reserva el derecho de auditar por sí o por terceros, las redes, tráfico y sistemas, equipos de cómputo y/o dispositivos de forma lógica o física para asegurar el cumplimiento de esta política sin importar la propiedad de este, siempre y cuando se encuentren dentro de las instalaciones o complejos de la APE o conectados a cualquier sistema de información, servicio de información o punto de infraestructura tecnológica.

- Todo usuario de los recursos tecnológicos del Estado, debe observar que existen restricciones en cuanto al empleo de software de terceros no autorizado, para la reproducción, transmisión o almacenamiento de música, videos, animaciones, imágenes, audio o cualquier otro tipo de información que no se refiera única y exclusivamente a los intereses y productividad relativa a sus funciones y responsabilidades. De acuerdo con este punto, se encuentra totalmente prohibido, la transmisión y/o recepción de audio, video, animaciones o cualquier otro tipo de información no autorizada en tiempo real.

- Con el fin de mantener la seguridad y la adecuada protección sobre virus informáticos y ofrecer soporte técnico necesario para las actividades de productividad de los usuarios, se prohíbe la instalación de software de terceros que no se encuentre específicamente autorizado por áreas de Infraestructura y Seguridad de TIC's de la DGTID.

Seguridad y Propiedad de la Información

- La interface de usuario para los sistemas de Internet/Intranet, o sistemas de información relacionados, debe estar clasificada como de uso confidencial, restringida o pública, tal y como se define en el *Estándar de Clasificación de Información*. Algunos ejemplos de información confidencial pueden ser, pero no limitada a: información privada, estrategias corporativas, secretos industriales, especificaciones técnicas de productos, lista de proveedores, directorios, datos de investigación, padrón detallado de contribuyentes, etc. Todos y cada uno de los empleados debe tomar todas las medidas necesarias para prevenir el acceso no autorizado a este tipo de información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Se debe mantener de forma segura, las claves de usuario y contraseña, así como no compartirlas con nadie por ningún medio. Los usuarios autorizados son los responsables por la seguridad y el uso de sus claves y cuentas. Las contraseñas deben modificarse periódicamente al menos cada seis meses.

- Todas las computadoras, laptops y estaciones de trabajo deben tener activo el protector de pantalla con contraseña por lo menos a los 10 minutos de detección de inactividad por parte del usuario o por el método de cerrar sesión cuando la estación no se encuentre atendida.

- Es necesaria la implementación del cifrado de la información de acuerdo con los estándares definidos y difundidos por la DGTID.

- Queda prohibido enviar cadenas o información a listas de correo o grupos de trabajo que no tengan relación expresa con las actividades motivo de sus obligaciones y responsabilidades.

- Tanto los empleados y/o servidores públicos, como los terceros que proporcionan sus servicios a la APE, deberán firmar sus mensajes enviados por correo electrónico, con al menos su nombre y el área a la que prestan sus servicios; y en su caso el teléfono en el cual es posible localizarles.

- Todos los equipos de cómputo empleados por el personal o servidores públicos de la APE, sea de propiedad de los usuarios o de las Dependencias y Entidades del Estado, deben ejecutar constantemente, el o los programas antivirus aprobados, verificar la legitimidad de sus aplicaciones y evitar intercambiar documentos e información por medio de dispositivos USB o memorias.

- Todo el personal usuario debe extremar precauciones al abrir archivos adjuntos recibidos desde orígenes desconocidos, los cuales podrían contener virus, bombas de correo o código tipo “caballo de troya” o malware. Cualquier situación deberá reportarse a la DGTID.

Uso Inaceptable de los Recursos Informáticos

- Las siguientes actividades están en términos generales, prohibidos. Por lo tanto, los servidores públicos, empleados de terceros y usuarios de la infraestructura informática

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

del Estado, deben sujetarse a las restricciones durante el cumplimiento de sus responsabilidades laborales. Por ejemplo, el personal de la DGTID, puede y debe inhabilitar el acceso a los recursos de red si cualquier estación interrumpe o perjudica los servicios de información. Por ninguna circunstancia, cualquier empleado o usuario estará autorizado para realizar actividades que se consideren ilegales bajo las leyes locales, federales o internacionales empleando los recursos tecnológicos y de información del Estado.

Actividades de Redes y Sistemas

Las siguientes actividades se encuentran totalmente prohibidas sin excepción alguna:

- Violar los derechos de cualquier persona o compañía protegida por los derechos de autor, secretos industriales, patentes o cualquier otra propiedad industrial de acuerdo con las leyes o regulaciones en la materia, la instalación o distribución de software "pirata" u otro tipo de software que no cuente con la respectiva licencia de uso autorizada.
- La copia no autorizada de material protegido por los derechos de autor, incluido, pero no limitado a la digitalización, distribución de fotografías, revistas, libros, o cualquier otra fuente de información protegida, música, así como la instalación de software protegido por los derechos de autor sin la licencia de uso correspondiente está totalmente prohibido.
- La introducción, transmisión y distribución intencional hacia la red de programas o código malicioso (virus, gusanos, caballos de troya, bombas de correo, etc.). Inclusive la habilitación de salida a internet por medio de proxys o herramientas ajenas a la DGTID.
- Revelar las cuentas de acceso a cualquier recurso informático o la autorización de uso de las cuentas personales por otros. Esto incluye expresamente a familiares y/o conocidos cuando se requiera el uso de recursos informáticos del uso y aprovechamiento de Tecnologías de la Información desde el hogar.
- El uso de los recursos del Estado para el almacenamiento, transmisión o distribución de material de contenido sexual o que incite a actos bélicos o delictivos.
- El ofrecimiento fraudulento de productos, bienes o servicios que se originen desde cualquier cuenta Institucional.
- El ofrecimiento de garantías de forma explícita o implícita a menos que formen parte de las responsabilidades de trabajo del personal que labora o tiene relación contractual con la DGTID o el Estado.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Ocasionar daños, perjuicios o interrupciones en los servicios de comunicaciones. Los aspectos de seguridad incluyen, pero no limitan a: el acceso a datos sin la autorización expresa del usuario o el acceso a servidores mediante la cuenta de un usuario sin autorización, a menos que se refiera a revisiones o auditorías que correspondan a las responsabilidades normales de trabajo de quien hace uso de cuentas de usuarios y por razones perfectamente justificadas. Para los propósitos de esta sección, "daños o perjuicios" incluye, pero no limita a las acciones de "husmeo" de la red, envío de paquetes de identificación (ping), envío de paquetes "spoofing" (simulación de paquetes internos o autorizados), acciones que provoquen denegación de servicios o manipulación de ruteo de información para propósitos maliciosos.
- El escaneo de puertos se encuentra expresamente prohibido a menos que se cuente con una notificación y autorización explícita de la *Dirección General de Tecnologías e Innovación Digital*.
- La ejecución de cualquier software o código de monitoreo de redes que tenga por objeto la intercepción de datos no autorizados por los usuarios a menos que esta actividad se encuentre dentro de las responsabilidades laborales de quien realiza el monitoreo de redes para fines de auditoría, análisis o revisión.
- Suplantar la identificación de cualquier usuario o sistema de seguridad ante cualquier estación, servidor o cuenta de servicio de información.
- Interferir o denegar cualquier servicio para cualquier usuario o empleado, como por ejemplo generar ataques de denegación de servicio de forma intencional o no intencional.
- El empleo de cualquier programa, script, software, instrucción o envío de mensajes que tengan por objeto, el intento de interferir o inhabilitar las sesiones de los usuarios a través de cualquier vía de servicio como Internet/Intranet de forma local o remota.
- Proporcionar información acerca de los empleados del uso y aprovechamiento de Tecnologías de la Información a terceros fuera del Estado de Oaxaca, sin consentimiento expreso y por escrito del propietario de la información y/o del proceso de información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

3.4 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por la Jefatura de la Unidad de Planeación y Control de TIC's, al menos una vez por año.

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Recurso Informático	Se refiere a computadoras, impresoras, laptops, escáner, fax, medios de comunicaciones, medios de transmisión de datos, sistemas de telefonía, unidades de almacenamiento, procesamiento y/o consulta de información y todo dispositivo que permita el registro, procesamiento, impresión, fotocopiado o transmisión de datos e información.
Uso apropiado	Empleo de los recursos informáticos, información y datos en tareas exclusivas para la administración y ejecución de las responsabilidades de la DGTID
Compromiso de seguridad	Pérdida, daño, alteración o disminución de las características de seguridad de la información que es integridad, confidencialidad y disponibilidad.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

CLASIFICACIÓN DE LA INFORMACIÓN

DIRECTRICES DE CLASIFICACIÓN

Referencia ISO 27001:2005. A.7 Gestión de Activos. A.7.2 Clasificación de Información.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión concluido***
A.7.2 A.7.2.1	Clasificación de Información Directrices de Clasificación	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Clasificación de la información.

Objetivo

Establecer los criterios de clasificación de la información propiedad y patrimonio de la APE

1.0 Propósito

Se definen los criterios de clasificación de la información con el objeto de delimitar cuando un conjunto de datos es de dominio público, restringido o altamente confidencial, incluyendo los datos personales de los contribuyentes, los cuales quedarán sujetos a la normatividad establecida y legislación vigente para tal efecto.

2.0 Ámbito de Aplicación

Este criterio aplica para todos los medios de información y datos que dispongan las Dependencias y Entidades del Estado y para los cuales se consideran medios impresos, digitales, sistemas de información, servicios de información, medios de almacenamiento

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

electrónico/digital y cualquier otro medio que represente piezas parciales o elementos completos de información propiedad o patrimonio del Estado.

Igualmente, el ámbito de la aplicación contempla a todas y cada una de las áreas y personas que laboran bajo cualquier modalidad laboral para la DGTID incluyendo a usuarios, proveedores y terceros que de cualquier forma tengan acceso físico y/o lógico a datos e información perteneciente la Administración Pública del Estado.

3.0 Política

3.1 Descripción de Política

- Todos los documentos generados dentro de para las Dependencias y Entidades del Estado, así como los reportes y/o consultas o pantallas de los sistemas de información, servicios de información y dispositivos de infraestructura de tecnología de para las Dependencias y Entidades del Estado deben contener la leyenda de clasificación de la información y clasificación de datos que para las Dependencias y Entidades del Estado defina.
- Cualquier documento, sistema de información, servicio de información o dispositivo de tecnología propiedad de la APE que no esté clasificado como restringido o confidencial de forma clara y explícita, será de uso y dominio público, entendiéndose este término para uso exclusivo de la APE.
- La información que se genera como parte del trabajo que los usuarios desempeñan dentro de APE, es propiedad exclusiva del Estado de Oaxaca, por ende, no puede ser divulgada o compartida y mucho menos usarse en beneficio económico propio del usuario.
- Para el cumplimiento de esta política, El Gobierno del Estado deberá considerar:

    - El estándar de clasificaciones de información de acuerdo con la normatividad vigente, así como los acuerdos o contratos de confidencialidad tanto con el personal de para las Dependencias y Entidades del Estado, como con usuarios, proveedores y terceros que tengan cualquier tipo de relación laboral, comercial, legal o de cualquier índole.

    - Los usuarios, se comprometen a no divulgar la información confidencial o restringida que pudiera obtener o manejar a través del acceso a sistemas o aplicaciones mediante su contraseña de acceso.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

El personal de la Jefatura de la Unidad de Planeación y Control de TICs de la Dirección de Servicios Tecnológicos debe ser responsable de la administración de las normas de seguridad del uso y aprovechamiento de Tecnologías de la Información, así como de la aplicación de los criterios de esta política para la instalación y configuración de los servicios, aplicaciones, accesos, protocolos, programas y sistemas requeridos por para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la creación y/o mantenimiento de documentos, así como a la generación de reportes, consultas o pantallas generados por los sistemas de información, servicios de información, o dispositivos de tecnología de la información empleados por parte de la DGTID

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado por la Jefatura de la Unidad de Planeación y Control de TIC's, al menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Personal responsable	Es la o las personas pertenecientes a la plantilla de operación del uso y aprovechamiento de Tecnologías de la Información, designadas para realizar actividades específicas tales como administración de sistemas, administración de seguridad o administración de bases de datos.
Servicio	Es el sistema, programa o software que proporciona servicios de información como: correo electrónico, nombre de dominio, servicio de páginas https, ftp, proxy y cualquier medio de software que permita el proceso, envío, recepción o redirección de información.
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Integridad	La información no debe ser alterada de tal forma que quede incompleta o incorrecta. A los usuarios no autorizados se les deben restringir los permisos para modificar o destruir información sensible.
Disponibilidad	La información debe ser accesible para usuarios autorizados en cualquier momento en que se necesite. La disponibilidad es una garantía de que la información pueda obtenerse en tiempo y frecuencia aceptable.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

CONFIDENCIALIDAD DE LA INFORMACIÓN

Referencia ISO 27001:2005. A.7 Gestión de Activos. A.7.2. Clasificación de Información. A.7.2.1. Directrices de clasificación

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.7.2 A.7.2.1	Clasificación de Información Directrices de clasificación	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Confidencialidad de la información.

Objetivo

Establecer los criterios de confidencialidad a los que estarán sujetos todo el personal, servidores públicos, proveedores y terceros de la APE.

1.0 Propósito

Definir los criterios de confidencialidad y uso de la información que se genere dentro de las instalaciones, complejos administrativos del Estado, a través del uso de la infraestructura tecnológica y del uso y aprovechamiento de Tecnologías de la Información y que debe aplicar para todo el personal que labora en la Administración Pública del Estado, así como para todos y cada uno de los proveedores, usuarios y terceros que tengan acceso a datos y/o información propiedad del Estado de Oaxaca.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Este criterio aplica para todos los medios de información y datos que dispongan las Dependencias y Entidades del Estado y para los cuales se consideran medios impresos, digitales, sistemas de información, servicios de información, medios de almacenamiento electrónico/digital, impresoras, fotocopiadoras, escáneres y cualquier otro medio que represente piezas parciales o elementos completos de información propiedad o patrimonio del Estado

Igualmente, el ámbito de la aplicación contempla a todas y cada una de las áreas y personas que colaboran bajo cualquier modalidad laboral para Estado, incluyendo a usuarios, proveedores y terceros que de cualquier forma tengan acceso físico y/o lógico a datos e información perteneciente la Administración Pública del Estado.

3.0 Política

3.1 Descripción de Política

Todo el personal, servidores públicos, que labora para el Estado así como, usuarios, proveedores y terceros, debe firmar un contrato de confidencialidad de información sin excepción.

- Todos los documentos generados dentro de para las Dependencias y Entidades del Estado, así como los reportes y/o consultas o pantallas de los sistemas de información, servicios de información y dispositivos de infraestructura de tecnología de para las Dependencias y Entidades del Estado, deben contener la leyenda de clasificación de la información y clasificación de datos que para las Dependencias y Entidades que la Administración de cada una defina y están sujetos al contrato de confidencialidad firmados por el personal que labora para La Administración Pública del Estado de Oaxaca , usuarios, proveedores y terceros.

- Toda la información generada, almacenada, procesada o consultada en medios y/o dispositivos físicos o lógicos dentro o en uso de infraestructura y por medios aprovechamiento de Tecnologías de la Información pertenece al Estado de Oaxaca, por lo tanto, es sujeta al contrato de confidencialidad.

- Por ningún motivo, el personal, servidores públicos del Estado de Oaxaca, usuarios, proveedores y terceros podrán hacer uso de la información para otros fines que no sean estrictamente los necesarios y relacionados con su operación y funciones. Lo anterior

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

incluye la impresión, transmisión, retransmisión, almacenamiento, procesamiento, extracción, copia, uso remoto o cualquier otro medio físico o lógico sin el permiso expreso del propietario del proceso y/o de la información y aplica para información, datos, piezas de información total o parcial.

- En caso de que exista el contrato con empresas, instituciones o entidades físicas o morales que presten sus servicios por cualquier medio al Estado, deberán estar sujetos al contrato de confidencialidad por sí y por las personas que a su vez laboran para ellos y que estén asignados a trabajos específicos dentro de la DGTID.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

El personal de la Dirección de Servicios Tecnológicos, debe ser responsable de la administración de las normas de seguridad del uso y aprovechamiento de Tecnologías de la Información, así como de la aplicación de los criterios de esta política para la instalación y configuración de los servicios, aplicaciones, accesos, protocolos, programas y sistemas requeridos por las Dependencias y Entidades del Estado, así como de los medios físico y/o lógicos donde se almacene, procese o consulte la información que pertenezcan la Administración Pública del Estado o que sean introducidos a las instalaciones del Estado de Oaxaca .

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC’s, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la creación y/o mantenimiento de documentos, así como a la generación de reportes, consultas o pantallas generados por los

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

sistemas de información, servicios de información, o dispositivos de tecnología de la información empleados por parte de la DGTID

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Jefatura de la Unidad de Planeación y Control de TIC´s, al menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Confidencial	Se aplica a lo que se hace o dice de manera reservada o secreta o con seguridad recíproca entre varias personas.
Información	Conjunto de datos sobre una materia determinada.
Dato	Información amplia o concreta que permite una deducción o conocimiento exacto.
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Término	*Definición*
Integridad	La información no debe ser alterada de tal forma que quede incompleta o incorrecta. A los usuarios no autorizados se les deben restringir los permisos para modificar o destruir información sensible. Debe ser completa, correcta y veraz.
Disponibilidad	La información debe ser accesible para usuarios autorizados en cualquier momento en que se necesite. La disponibilidad es una garantía de que la información pueda obtenerse en tiempo y frecuencia aceptable.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID.*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

PROTECCIÓN DE LA INFORMACIÓN

Referencia ISO 27001:2005. A.7 Gestión de Activos. A.7.2 Clasificación de la Información. A.7.2.2. Etiquetado y manipulado de la información

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.7.2	Clasificación de la Información			
A.7.2.2	Etiquetado y manipulado de la información	2	2.0	En revisión
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Protección de la información.

Objetivo

Establecer controles de protección de la información durante el uso y aprovechamiento de las Tecnologías de la Información y Comunicaciones.

1.0 Propósito

Establecer controles mínimos de seguridad en el tratamiento de la información, limitando las fugas incontroladas y permitir la detección de éstas en caso de que se produzcan, a través de una serie de precauciones.

2.0 Ámbito de Aplicación

Este control aplica para todos los medios de información y datos de que disponga La Administración Pública del Estado de Oaxaca y para los cuales se consideran medios impresos, digitales, sistemas de información, servicios de información, medios de almacenamiento

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

electrónico/digital copiadoras, impresoras, escáneres y cualquier otro medio que represente piezas parciales o elementos completos de información propiedad o patrimonio del Estado

Igualmente, el ámbito de la aplicación contempla a todas y cada una de las áreas y personas servidores públicos, que laboran bajo cualquier modalidad para la Administración Pública del Estado, incluyendo a usuarios, proveedores y terceros que de cualquier forma tengan acceso físico y/o lógico a datos e información perteneciente la Administración Pública del Estado.

3.0 Política

3.1 Descripción de Política

- Toda la información de las Entidades y Dependencias del Estado, debe ser protegida de acuerdo a su confidencialidad, valor y criticidad, con medios técnicos y legales de accesos no autorizados, de forma que se evite, en la medida de lo posible, que cualquier persona física o jurídica pueda acceder/obtener/tratar/difundir/o persuadir con la misma fraudulenta o ilícitamente, no importando el medio o ubicación en donde la información este guardada, procesada por sistemas tecnológicos o administrada por el personal o usuarios. Esta política promueve la revisión en que la información fluye a través de las áreas de la *Dirección General de Tecnologías e Innovación Digital*.
- La información *que sea* propiedad del Estado, debe ser utilizada únicamente para los propósitos de operación y gestión de negocio expresamente definidos por sus atribuciones; por lo que están prohibidos todos los usos no autorizados de la información para fines personales cualesquiera que estos sean.
- La Información de Entidad de la APE, debe tener designado un propietario responsable de determinar las clasificaciones correspondientes a la confidencialidad y la criticidad, tomando decisiones y el control documentando de quien tiene acceso, garantizando que se tienen los controles suficientes y adecuados en el almacenamiento, manejo distribución y uso regular de la información.
- Queda prohibida la divulgación por cualquier medio de toda la información del Estado, específicamente la clasificada como “Información Crítica”;
- Toda la información del Estado, deberá ser etiquetada de acuerdo a las normas emitidas por su cada área de la APE “Información Crítica o Confidencial”.
- La información clasificada como “Confidencial” debe contar con una protección especial, tendente a evitar su filtración, divulgación o difusión a terceros, acciones que pueden causar graves perjuicios. Limitar su acceso, permitiendo el acceso a dicha información sólo al personal que por razón de su cargo o funciones es necesario que acceda a dicha información, no permitiendo tal acceso al resto del personal.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- La información de carácter crítica, así como el software y aplicaciones definidas como críticas, debe respaldarse de acuerdo a los procedimientos y periodicidad indicados por la DGTID. El tratamiento de resguardo de esta información deberá conservarse cuando menos cinco años.
- La integridad de la información sensible, critica o valiosa almacenada por largos periodos de tiempo, debe estar garantizada por procedimientos de validación de la misma.
- Queda prohibida la enajenación, de toda la información del Estado.
- Se prohíbe la reproducción parcial o total y por cualquier método o medio, sin autorización expresa y por escrito de las Direcciones Jurídicas de cada Entidad o Dependencia.
- Las personas que alteren cualquier información del Estado, para su beneficio o perjuicio o beneficio de un tercero, serán sancionadas conforme a lo dispuesto en las Leyes correspondientes.
- Cuando ya no sea necesaria la información sensible o valiosa esta debe ser destruida de manera segura, utilizando los procedimientos autorizados por cada Dirección Administrativa. Los procedimientos para la destrucción de la información deberán alinearse a la Norma que para tal fin se encuentra documentada en el SGSI de la Dirección de Servicios Tecnológicos.
- Cuando la información del Estado que se resguarde en infraestructura tecnológica en custodia de la DGTID sufra un Siniestro por causas ajenas o imprevisibles, como son los desastres naturales, y que como consecuencia la información sufra cualquier tipo de daño o perdida, para tener conocimiento de los hechos, la DGTID, se apoyara de la Unidad administrativa de Asuntos Jurídicos de la Dependencias afectada dentro de los 10 días naturales posteriores al evento, anexando el Acta de hechos y/o Acta Administrativa que debe contar con la firma del representante del Órgano Interno de Control.
- Cuando la información sea móvil de robo, uso o explotación indebida por cualquier persona, medio o cualquier hecho delictivo, para tener conocimiento de los hechos la *Dirección General de Tecnologías e Innovación Digital se apoyará de la Dirección de* Asuntos Jurídicos en cuanto se detecte el ilícito, procediendo alternadamente al aviso a las autoridades para el correspondiente Acta de Levantamiento de hechos y/o Acta Administrativa que debe contar con la firma del representante de la Contraloría.
- En el supuesto que el incidente lo cometa un empleado de un tercero prestador de servicios, además de las autoridades señaladas en el punto anterior la *Dirección General de Tecnologías e Innovación Digital*, emitirá un informe del mismo acto y por escrito al prestador de servicios, con la finalidad de proceder jurídicamente en los términos del contrato de prestación de servicios en la causal de responsabilidad del tercero prestador de servicios por su personal asignado.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- LA DGTID deberá establecerá Acuerdos o Pactos de Confidencialidad con el personal que labora en el APE, proveedores, terceros prestadores de servicios, etc., a fin de permitir proteger la información confidencial, estableciendo expresamente las obligaciones y limites que se han de tener en cuenta en su tratamiento, debiendo informar las consecuencias que pueden derivarse del incumplimiento de dicha obligación de confidencialidad y secreto. Así, puede establecerse que la sustracción o revelación de dicha información puede ser constitutivo de un ilícito de naturaleza penal.
- La DGTID establecerá medidas técnicas que permitan la visualización o tratamiento de información confidencial (por ejemplo: uso de contraseñas para el acceso a los documentos, cifrado (criptografía) etc.).
- La DGTID en la medida de los posible debe Mantener/Almacenar los documentos confidenciales en soporte papel, que son de su incumbencia, en archiveros o lugares que se encuentren cerrados bajo llave o cajas fuertes, a las que sólo tengan acceso las personas autorizadas.
- La DGTID Realizará conforme a los recursos disponibles copias de seguridad de los sistemas que tenga bajo su custodia, que eviten la pérdida de información confidencial o sensible en caso de catástrofe.
- La DGTID deberá establecer acuerdos con los terceros en función de su obligación de devolver la información confidencial a la que se ha tenido acceso en el momento que termine la relación contractual con la DGTID, estableciendo que, a pesar de dicha terminación, la obligación de confidencialidad y secreto permanecerá vigente durante el plazo que sea establecido por las partes.
- Efectuar campañas de difusión a las Entidades y Dependencias de la APE, sobre la importancia de la seguridad y control en el tratamiento de la información,
- La *Dirección General de Tecnologías e Innovación Digital* mediante sus controles, debe garantizar que la información de la Dirección está protegida con procesos que mantienen la confidencialidad, la integridad y la disponibilidad de la información de los sistemas que se manejan.

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

El personal de la *Dirección General de Tecnologías e Innovación Digital* debe ser responsable de la administración de las normas de seguridad del uso y aprovechamiento de Tecnologías de la Información, así como de la aplicación de los criterios de esta política para la instalación y configuración de los servicios, aplicaciones, accesos, protocolos, programas y sistemas requeridos por para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TICs, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la creación y/o mantenimiento de documentos, así como a la generación de reportes, consultas o pantallas generados por los sistemas de información, servicios de información, o dispositivos de tecnología de la información empleados por parte de la DGTID

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por *la Dirección General de Tecnologías e Innovación Digital* a través del personal autorizado en el uso y aprovechamiento de Tecnologías de la Información al menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad*.**

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Término

Término	*Definición*
Confidencial	Se aplica a lo que se hace o dice de manera reservada o secreta o con seguridad recíproca entre varias personas.
Información	Conjunto de datos sobre una materia determinada.
Dato	Información amplia o concreta que permite una deducción o conocimiento exacto.
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Integridad	La información no debe ser alterada de tal forma que quede incompleta o incorrecta. A los usuarios no autorizados se les deben restringir los permisos para modificar o destruir información sensible. Debe ser completa, correcta y veraz.
Disponibilidad	La información debe ser accesible para usuarios autorizados en cualquier momento en que se necesite. La disponibilidad es una garantía de que la información pueda obtenerse en tiempo y frecuencia aceptable.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

ANTES DEL EMPLEO

TÉRMINOS Y CONDICIONES DE CONTRATACIÓN

Referencia ISO 27001:2005. A.8 Seguridad ligada a los Recursos Humanos A.8.1 Antes del empleo.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.8.1 A.8.1.3	Antes del empleo Términos y condiciones de contratación	2	2.0	Concluido
Vigencia a partir de:		**Marzo 2019**		

Título de la política

Establecer los términos y condiciones de contratación que los empleados, contratistas y terceros, deben aceptar y firmar, detallando las responsabilidades de ellos y de la DGTID para lograr la seguridad de la información.

Objetivo

Establecer la obligatoriedad para que él o las áreas de Recursos Humanos consideren en el contrato los términos y condiciones que se exponen en esta política.

1.0 Propósito

Garantizar que los empleados, contratistas y terceros, y Unidades Administrativas de la APE, tengan claras sus responsabilidades con la finalidad de proteger y mantener la seguridad en la información patrimonio del Estado.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

El ámbito de la aplicación contempla a todas las personas que laboran bajo cualquier modalidad laboral dentro de la Administración Pública del Estado, incluyendo a empleados, servidores públicos, usuarios, proveedores y terceros que de cualquier forma tengan acceso físico y/o lógico a datos e información perteneciente a la Administración Pública del Estado.

3.0 Política

3.1 Descripción de Política

- Para usuarios, proveedores y terceros, su Director de área, o Patrón (en el caso de proveedores), deberán firmar un acuerdo de confidencialidad o no divulgación, antes de otorgarles algún acceso físico al área donde laborarán y previo a tener acceso a la información y a los medios de procesamiento de la misma.
- Los términos y condiciones del acceso deben establecer los términos, vigencia, y alcance para ser otorgados.
- Los derechos y obligaciones de los empleados, usuarios, proveedores y terceros, relativos a la seguridad de la información, relacionados con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de su respectivo contrato o especificaciones técnicas.
- Los detalles técnicos de los sistemas de información, tales como direcciones de redes, diagramas de redes, software de seguridad utilizado, etc., no deben ser revelados a los aspirantes al empleo ni a proveedores mientras no hayan firmado el acuerdo de confidencialidad y hayan sido empleados o contratados.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

La Dirección de Servicios Tecnológicos, deberá ser responsables de la administración y cumplimiento de la presente política, así como de la aplicación de los criterios necesarios para

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

preservar los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, de reglamentos, jurídicos, financieros o de cualquier otra índole incluyendo los avances tecnológicos que tengan impacto en las facultades del área de Recursos Humanos, la Dirección de Administración y la *Dirección General de Tecnologías e Innovación Digital*.

3.4 Revisiones y auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por la Dirección General de Tecnologías e Innovación Digital al personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad***.

Los servicios de auditoría al Sistema de Gestión de la Seguridad de la Información (SGSI), o a cualquier otro elemento de gestión de tecnología deberá ser efectuado por entidades externas a para las Dependencias y Entidades del Estado por lo menos una vez al año.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

5.0 Revisiones Históricas de la Política

Término	***Definición***
Confidencialidad	La información crítica o sensible debe estar disponible únicamente para un conjunto definido de personas. La transmisión no autorizada, así como el uso de información debe estar restringida.
Integridad	La información no debe ser alterada de tal forma que quede incompleta o incorrecta. A los usuarios no autorizados se les deben restringir los permisos para modificar o destruir información sensible. Debe ser completa, correcta y veraz.
Disponibilidad	La información debe ser accesible para usuarios autorizados en cualquier momento en que se necesite. La disponibilidad es una garantía de que la información pueda obtenerse en tiempo y frecuencia aceptable.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

CESE DEL EMPLEO O CAMBIO DE PUESTO DE TRABAJO

NOTIFICACIÓN SOBRE MOVIMIENTOS LABORALES A LA DIRECCIÓN DE SERVICIOS TECNOLÓGICOS

Referencia ISO 27001:2005. A.8 Seguridad ligada a los Recursos Humanos A.8.3 Cese de empleo o cambio de puesto de trabajo.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.8.3 A.8.3.2 A.8.3.3	Cese de empleo o cambio de puesto de trabajo Devolución de activos Retirada de los derechos de acceso	2	2.0	Programado
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Notificación a las áreas de negocio de la APE sobre movimientos laborales del personal de la Dirección General de Tecnologías e Innovación Digital.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Objetivo

Notificar a las áreas administrativas o de negocio de las Dependencias de la APE, de los cambios, altas, bajas, del personal de la DGTID, con el propósito de garantizar la continuidad de servicios.

1.0 Propósito

Garantizar que los cambios o movimientos laborales del personal adscrito a la DGTID no impacten en la provisión de servicios. Cualquier movimiento de las áreas administrativas de la Dirección General de Tecnologías e Innovación Digital, deberá ser notificado sin excepción al enlace o áreas de negocio con el objeto de que se establezcan los mecanismos de continuidad operativa sin contratiempo alguno.

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para la Dirección de Servicios Tecnológicos a fin de notificar oportunamente a las áreas de negocio.

- Para todas y cada una de las áreas operativas de la DGTID
- Al acceso a todos los sistemas de información, infraestructura tecnológica en custodia de la DGTID:

3.0 Política

3.1 Descripción de Política

- La DGTID a través de la Dirección de Servicios Tecnológicos deberá reportar o notificar a las áreas usuarias de la APE; y en su caso a las áreas de recursos humando de todos y cada uno de los cambios del personal en cuanto a, permisos, amparos, vacaciones, coberturas, renuncias, despidos y cualquier otro tipo de movimiento, con el objeto de ejecutar algunas de las siguientes acciones que apliquen a cada caso.
    - Creación de cuentas y/o perfiles de usuario para acceso a los sistemas de información, servicios de información y/o uso de la infraestructura tecnológica en administración y custodia de la DGTID.
    - Modificación de cuentas o perfiles de usuario.
    - Inhabilitación de cuentas y/o perfiles de usuario.
    - Respaldos de información, cuentas y/o perfiles de usuario.
    - Recuperación de respaldos de información, cuentas y/o perfiles de usuario.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

DEVOLUCIÓN DE ACTIVOS

- Con la finalidad de efectuar la devolución de activos, para niveles de Jefe de Departamento de la Dirección General de Tecnologías e Innovación Digital hacia arriba se deberá proceder mediante Acta de Entrega-Recepción vs. Anexo respectivo de capítulo de Acta y Certificado de no adeudo.
- Para Terceros prestadores de servicio, la devolución de activos se cumple mediante los requisitos para baja de recurso (Carta de Entrega para Terceros Prestadores de Servicio).

RETIRADA DE LOS DERECHOS DE ACCESO

- Notificación al usuario, de la creación y/o modificación de cuentas o perfiles para el acceso a los sistemas de información, servicios de información o uso de la infraestructura tecnológica.
- Notificación de la Dirección General de Tecnologías e Innovación Digital y/o a la Dirección de Servicios Tecnológicos al o las áreas de Recursos Humanos, sobre la creación, modificación, retirada o cancelación de los accesos a los sistemas de información, servicios de información o uso de la infraestructura tecnológica. Por lo que los derechos de acceso a la información y a los recursos de tratamiento de información de todos los empleados, contratistas y/o terceros, serán retirados a la finalización del empleo, contrato y/o acuerdo o bien, serán adaptados a los cambios producidos.
- Las notificaciones deberán apegarse a la forma y formato que para tal efecto establezca el área de Recursos Humanos de común acuerdo con la Dirección General de Tecnologías e Innovación Digital.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

La Dirección General de Tecnologías e Innovación Digital, debe ser responsables de la administración y cumplimiento de la presente política, así como de la aplicación de los criterios necesarios para preservar los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, de reglamentos, jurídicos, financieros o de cualquier otra índole incluyendo los avances tecnológicos que tengan impacto en las facultades del área de Recursos Humanos, la Dirección de Administración y la Dirección de Servicios Tecnológicos.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad***.

Los servicios de auditoría al Sistema de Gestión de la Seguridad de la Información (SGSI), o a cualquier otro elemento de gestión de tecnología deberá ser efectuado por entidades externas a para las Dependencias y Entidades del Estado por lo menos una vez al año.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca,

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Recursos Humanos	El área administrativa facultada para autorizar cualquier movimiento laboral del personal del uso y aprovechamiento de Tecnologías de la Información
Usuario	Persona que utiliza los sistemas informáticos de la DGTID al que se le ha proporcionado una "Cuenta de usuario asociada a una contraseña", siendo estos administrados por el Directorio Activo de la DGTID. Por lo que en el APE no existe la figura de "Usuario" que no tenga acceso al uso de internet o correo electrónico.
Sistema de información	Sistema o medio informático que almacene, procese o recupere información.
Servicio de información	Sistema, software, programa o rutina que permita el almacenamiento, procesamiento, recuperación o retransmisión de información.
Infraestructura tecnológica	Sistemas de información, servicios de información, software, programas, rutinas, dispositivos, sistemas de comunicaciones, sistemas de transmisión de voz y/o datos y cualquier otro medio eléctrico, electrónico o impreso propiedad de la DGTID
Propiedad	Cualquier tipo de hardware o software que el uso y aprovechamiento de Tecnologías de la Información tenga en propiedad, copropiedad, arrendamiento, subarrendamiento, préstamo, donación o cualquier otra forma en que el goce de los derechos esté a favor de la DGTID

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

SEGURIDAD FÍSICA Y AMBIENTAL

ÁREAS SEGURAS

Referencia ISO 27001:2005. A.9 Seguridad Física y Ambiental A.9.1 Áreas Seguras.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.9.1	Áreas Seguras	2	2.0	Concluido
A.9.1.1	Perímetro de seguridad física			
A.9.1.2	Controles físicos de entrada			
A.9.1.3	Seguridad de oficinas, despachos e instalaciones			
A.9.1.4	Protección contra las amenazas externas y de origen ambiental	1	1.0	Concluido
A.9.1.5	Trabajo en áreas seguras			
Vigencia a partir de:		Marzo 2019		

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Título de la Política

Promover y mantener la seguridad y salud humana en las áreas de trabajo.

Objetivo

Evitar el acceso físico no autorizado a inmuebles y centros de administración de datos y áreas críticas de TI en administración custodia de la DGTID; evitado el daño e interferencia con la información y los inmuebles de la Dirección General de Tecnologías e Innovación Digital, así como mantener la seguridad y salud humana en las áreas de trabajo de la DGTID.

1.0 Propósito

Garantizar que las áreas de trabajo, centros de datos e información crítica que forman parte de la Dirección General de Tecnologías e Innovación Digital cuentan con las medidas de seguridad y salud humana adecuadas, promoviendo la consciencia entre el personal para conservar, mantener dichas medidas.

Garantizar que las áreas de trabajo y de entrega de servicios de la DGTID cuentan con las medidas de protección para la salud humana, la seguridad física y la integridad de la información en apego a las disposiciones en materia de Salud Pública que dicten las autoridades del Estado, así como a las políticas de seguridad de la información que emita la DGTID. Estas medidas se deberán promover por medios digitales para que los usuarios y público en general conozcan y tomen conciencia de ellas.

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para todo el personal de la DGTID y del personal o usuarios que tienen acceso a los sistemas de información, servicios de información, infraestructura tecnológica ubicados, en propiedad, copropiedad, arrendados, subcontratados, o que, por cualquier otro medio, pertenezcan a la Dirección General de Tecnologías e Innovación Digital. En el despliegue de servicios de la DGTID para todos los usuarios dentro de los complejos administrativos de la APE, así como las posiciones remotas como radio bases y centros operativos para la atención de la ciudadanía.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.0 Política

3.1 Descripción de Política

PERÍMETRO DE SEGURIDAD FÍSICA

- La Dirección General de Tecnológicos e Innovación Digital., deberá prever la existencia de perímetros de seguridad para proteger las áreas que contienen las instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información y plataforma tecnológica que tenga bajo su administración y custodia.

- De acuerdo con el análisis de riesgos efectuado, se definirá y documentará claramente un perímetro de seguridad física adecuado para salvaguardar las instalaciones que resguardan la infraestructura tecnológica, sobre todo las que albergan los Centros de Datos y la información vital del Estado de Oaxaca.

- Se deberán identificar claramente todas las salidas de emergencia del perímetro de seguridad.

- Extender las barreras físicas necesarias del Centro de Datos desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental tales como, humedad, fauna, inundación e incendio.

CONTROLES FÍSICOS DE ENTRADA

- El acceso a las áreas y edificios donde se encuentren los centros de datos de la Dirección General de Tecnologías e Innovación Digital deberán estar restringidas. Exclusivamente personal autorizado podrá tener acceso, registrando cada ingreso y egreso en forma precisa ya sea en primera instancia, mediante un área de recepción atendida por personal y/o por mecanismos de registro electrónico.

- Las puertas de acceso a las áreas restringidas deberán permanecer cerradas. Solo tendrán acceso a dichas áreas el personal debidamente autorizado y en caso estrictamente necesario.

- Debe cumplirse el procedimiento para ingresar, permanecer y retirarse de las instalaciones de la Dirección General de Tecnologías e Innovación Digital y de los centros de datos, con la finalidad de resguardar y proteger físicamente el acceso no autorizado o

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

daño a los activos de tecnología de información de la Dirección General de Tecnologías e Innovación Digital. El ingreso debe ser lo suficientemente justificado.

- Los visitantes o personal ajeno a las instalaciones de la Dirección General de Tecnologías e Información Digital, deberán seguir el procedimiento para ingresar, permanecer y retirarse de las instalaciones, registrando su entrada a las instalaciones en la recepción de dichos edificios, por el personal de vigilancia mediante el intercambio de **gafete de visitante,** por una identificación oficial vigente (INE, Pasaporte o Licencia de Conducir), este gafete deberá portarlo en un lugar visible, durante toda su permanencia en las instalaciones. El personal de vigilancia verificará con el personal con facultades para autorizar, la posibilidad de permitir o no el acceso a las instalaciones. De permitirse el acceso, deberá ser escoltado hasta el lugar donde reside el personal que lo recibirá.

- Todos los maletines, maletas, carteras y demás equipajes deben ser abiertos, para que el personal de seguridad los revise al momento de la entrada.

- Revisar y actualizar periódicamente, los derechos de acceso a las áreas restringidas, los que serán documentados y debidamente autorizados.

- Cuando un trabajador termina su relación laboral con la APE, todos los derechos de acceso a las áreas restringidas del mismo deberán ser revocados inmediatamente, así como también todos los códigos de seguridad para el acceso físico conocidos o disponibles al ex-trabajador, deben ser desactivados.

SEGURIDAD DE OFICINAS, DESPACHOS E INSTALACIONES

- Todos los empleados de la Dirección General de Tecnologías e Innovación Digital con oficinas propias separadas deben cerrar sus puertas con llave cuando las oficinas no estén en uso.

- El acceso a toda oficina, Centro de Datos y área de trabajo que contenga información sensible debe ser físicamente restringido para limitar el acceso.

- Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Ubicar las funciones y el equipamiento de soporte tales como: impresoras, fotocopiadoras, máquinas de fax, etc., adecuadamente dentro del área protegida para evitar acciones que puedan comprometer la información.

- Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.

- Mediante las cámaras de circuito cerrado se efectuará el control para la detección de intrusos. Dichos mecanismos deberán ser probados periódicamente con el fin de corroborar su buen funcionamiento. Estos mecanismos de control deberán comprender todas las puertas exteriores y ventanas accesibles.

- Se deberá adoptar la política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

- Se deberá almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

- Se deberá guardar bajo llave la información sensible o crítica de la APE cuando no está en uso, especialmente cuando no hay personal en la oficina.

- Se deberá desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante contraseñas u otros controles cuando no están en uso.

- Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

TRABAJO EN ÁREAS SEGURAS Y SEGURIDAD EN EL CENTRO DE DATOS

- Con la finalidad de establecer e incrementar la seguridad de las áreas protegidas o restringidas, estas deberán darse a conocer al personal, con la finalidad de que acaten las políticas y procedimientos para el acceso a las mismas, en caso de requerirlo.

- Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso como el de cualquier otra persona ajena que requiera acceder a estas áreas, será otorgado solamente cuando sea necesario y si se encuentra autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

- El acceso físico al Centro de Datos es restringido, únicamente será dará acceso para el personal autorizado o que labore en dichas instalaciones y bajo estricta necesidad. No están permitidas las visitas sin motivo o causa real que lo amerite, la distribución, inventarios, y arreglos tecnológicos pueden ser consultados por medios remotos.

- Se deberá evitar la ejecución de trabajos por parte de terceros sin supervisión.

- En caso estrictamente necesario de acceso, se deberá impedir a cualquier persona ajena al Centro de Datos, el ingreso y la utilización de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información.

- Se deben colocar señalamientos en el Centro de Datos para indicar la ubicación de extintores manuales y salidas de emergencia.

- Está terminantemente prohibido comer, beber, fumar y encender fuego o desarrollar actividades que comprometan la integridad física de los equipos, mobiliario o de los usuarios dentro de las instalaciones a cargo y custodia de la DGTID.

- No debe existir material explosivo y/o flamable dentro de las instalaciones del Centro de Datos.

- Deberá efectuarse limpieza y mantenimientos preventivos periódicos a las instalaciones del Centro de Datos, estableciendo las ventanas de mantenimiento, así como el registro de los resultados de dichos procedimientos.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- El Centro de Datos y el área de Telecomunicaciones deben contar con una bodega independiente, para almacenar equipo de cómputo y/o telecomunicaciones, así como, suministros.

- No está permitido en ninguna circunstancia el acceso a las instalaciones fuera de las horas de acceso y trabajo autorizadas, a menos que se tenga la autorización respectiva o en el caso del Centro de Datos, ocurra alguna contingencia.

- Se deben contemplar y poner en marcha los procedimientos en caso de contingencias o eventualidades con la finalidad de proteger la seguridad del personal y salvaguardar las instalaciones.

- Capacitar y adiestrar al personal de la Dirección General de Tecnologías e Innovación Digital, por lo menos una vez al año con respecto a los procedimientos en caso de contingencias o eventualidades, así como, realizar simulacros de evacuación por lo menos una vez al año.

PROTECCIÓN DE LA SALUD EN LOS COMPLEJOS ADMINISTRATIVOS DE LA APE

- El personal de la DGTID deberá acatar puntualmente las disposiciones en materia de salud pública emitidas por las Autoridades del Estado, debiendo notificar cualquier afectación física que ponga en riesgo su salud o la de sus compañeros de trabajo.

- Todo el personal de la DGTID, durante la provisión y entrega de servicios, deberá portar además de sus herramientas de trabajo, el equipo de protección personal que recomienden y dicten las autoridades de Salud Pública del Estado.

- La DGTID protege el bienestar y la salud de sus colaboradores, por lo que, el personal de tercera edad, con problemas crónicos de salud, y embarazadas, tendrán, en apego a la legislación y normativa aplicable, así como a las disposiciones de salud pública que emitan las autoridades de salud Estatal, las facilidades de trabajo en remoto en situaciones que pongan en riesgo su salud e integridad física como: Pandemias, desastres naturales o conflictos sociales.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

El personal de las áreas de Recursos Humanos y de la Dirección General de Tecnologías e Innovación Digital, deben ser responsables de la administración y cumplimiento de la presente política, así como de la aplicación de los criterios necesarios para preservar los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

3.3 Monitoreo

Se deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, de reglamentos, jurídicos, financieros o de cualquier otra índole incluyendo los avances tecnológicos que tengan impacto en las facultades del área de Recursos Humanos, la Dirección de Administración y la Dirección de Servicios Tecnológicos.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones. Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad***.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Los servicios de auditoría al Sistema de Gestión de la Seguridad de la Información (SGSI), o a cualquier otro elemento de gestión de tecnología deberá ser efectuado por entidades externas a para las Dependencias y Entidades del Estado por lo menos una vez al año.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Recursos Humanos	El área administrativa facultada para autorizar cualquier movimiento laboral del personal del uso y aprovechamiento de Tecnologías de la Información
Usuario	Persona que utiliza los sistemas informáticos de la DGTID al que se le ha proporcionado una "Cuenta de usuario asociada a una contraseña", siendo estos administrados por el Directorio Activo de la DGTID. Por lo que en el APE no existe la figura de "Usuario" que no tenga acceso al uso de internet o correo electrónico.
Infraestructura tecnológica	Sistemas de información, servicios de información, software, programas, rutinas, dispositivos, sistemas de comunicaciones, sistemas de transmisión de voz y/o datos y cualquier otro medio eléctrico, electrónico o impreso propiedad de la DGTID
Propiedad	Cualquier tipo de hardware o software que el uso y aprovechamiento de Tecnologías de la Información tenga en propiedad, copropiedad, arrendamiento, subarrendamiento, préstamo, donación o cualquier otra forma en que el goce de los derechos esté a favor de la DGTID
UPS	Unidad de Energía Interrumpible

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

SEGURIDAD DE LOS EQUIPOS

Referencia ISO 27001:2005. A.9 Seguridad Física y Ambiental A.9.2 Seguridad de los equipos

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.9.2	Seguridad de los equipos	2	2.0	En proceso
A.9.2.1	Emplazamiento y protección de equipos			
A.9.2.2	Instalaciones de suministro			
A.9.2.3	Seguridad del cableado			
A.9.2.4	Mantenimiento de los equipos			
A.9.2.5	Seguridad de los equipos fuera de las instalaciones			
A.9.2.6	Reutilización o retirada segura de equipos			
Vigencia a partir de:		Marzo 2019		

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Título de la Política

Promover y mantener la seguridad física de los equipos

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con los equipos de la DGTID.

1.0 Propósito

Garantizar que los equipos en administración custodia de la Dirección General de Tecnologías e Innovación Digital, cuenten con las medidas de seguridad física adecuadas, promoviendo la consciencia entre el personal para conservar, mantener dichas medidas.

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para todo el personal, servidores públicos, y usuarios que tiene acceso a los sistemas de información, servicios de información, infraestructura tecnológica ubicados, en propiedad, copropiedad, arrendados, subcontratados, o que, por cualquier otro medio, administre y custodie la DGTID.

3.0 Política

3.1 Descripción de Política

EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS.

- Los equipos que contienen información crítica de áreas sustantivas de operación y de negocio dela APE, deberán estar situados en un área especial tal como el Centro de Datos del Estado, de forma que se reduzcan los riesgos derivados de las amenazas y peligro de origen ambiental y social.

- Todos los equipos deberán contar con controles para evitar accesos no autorizados.

- La Dirección de Servicios Tecnológicos deberá estar atenta de que funcionen adecuadamente los sistemas de prevención y supresión de incendios, aire acondicionado, control de humedad y otros sistemas de protección de ambientes computarizados, en el

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Centro de Datos. Debiendo informar oportunamente cualquier situación que los ponga en riesgo.

INSTALACIONES DE SUMINISTRO.

- El Centro de Datos deberá contar con un sistema de emergencia de suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Estado de Oaxaca.

- El Plan de Recuperación en casos de Desastre (DRP) deberá contemplar las acciones que han de emprenderse ante una falla de la UPS.

- La UPS será inspeccionada y probados periódicamente para asegurar que funciona correctamente y que tienen la autonomía requerida.

SEGURIDAD DEL CABLEADO

- El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información deberá estar protegido contra intercepción o daño.

- Deberán estar separados los cables de energía de los cables de comunicaciones para evitar interferencias y lograr una adecuada identificación de estos.

- La instalación y el mantenimiento de los cables de electricidad y de comunicaciones deben ser efectuados por especialistas en el ramo, cumpliendo las normas establecidas de seguridad para tal fin.

MANTENIMIENTO DE LOS EQUIPOS

- Deberá efectuarse periódicamente mantenimiento preventivo de todos los equipos de computación y comunicación.

- Todos los equipos que albergan sistemas de información utilizados en el proceso de producción deben conservarse de acuerdo con las especificaciones e intervalos de servicio recomendadas por el proveedor, con reparaciones y servicios ejecutados solamente por personal de mantenimiento calificado y autorizado.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Se realizará el mantenimiento preventivo de los equipos de cómputo para asegurar su disponibilidad e integridad permanentes.

- Sólo personal de mantenimiento autorizado deberá brindar el mantenimiento preventivo y correctivo de los equipos de cómputo.

- Deberán quedar registradas todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado, así como también aquel equipo que es necesario retirar de las instalaciones de la APE para su mantenimiento.

- Para el caso de mantenimiento preventivo, se realiza notificación mediante el oficio de los periodos programados, con la finalidad de que los usuarios realicen el respaldo correspondiente que a su criterio sea necesario.

- Para mantenimiento correctivo, este se realiza en presencia de los usuarios, conforme a programación de solicitud levantada en Mesa de servicio.

- En caso, de qué el mantenimiento correctivo de algún elemento de Hardware y Software presenten alguna falla, se procederá a efectuar respaldo de protección (autorizado por el usuario), para atención de la solución del servicio.

SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

- El uso de los equipos de la Dirección de Servicios Tecnológicos fuera de las instalaciones del edificio anexo de la Dirección General de Tecnologías e Innovación Digital, debe ser debidamente autorizado por el titular de la misma.

- Se deberán aplicar las medidas de seguridad a los equipos situados fuera de las instalaciones de APE y equipos móviles que se conectan a la red de Dirección General de Tecnologías e Innovación Digital.

- Se deberá contar con un inventario de los equipos situados fuera de las instalaciones de APE y equipos móviles que se conectan a la red de la Dirección General de Tecnologías e Innovación Digital.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

REUTILIZACIÓN O RETIRADA SEGURA DE LOS EQUIPOS

- Con la finalidad de reutilizar o retirar de forma segura los equipos, todos los soportes de almacenamiento se deberán revisar para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han reinstalado de manera segura, antes de su retirada.

- Los equipos de cómputo y/o telecomunicaciones de las oficinas de la Dirección General de Tecnologías e Innovación Digital, no deben ser trasladados o reubicados sin la previa autorización y conocimiento de la Dirección de Servicios Tecnológicos.

- Con la finalidad de efectuar la retirada segura de los equipos de cómputo y/o telecomunicaciones, estos deberán registrarse en el SATI (Sistema de Administración de Accesos de Tecnología de Información) en la recepción del edificio Anexo de la Dirección General de Tecnologías e Innovación Digital para la entrada o salida del mismo, según el "Procedimiento de Control de Acceso al Edificio de Tecnología de la Información (Edificio Anexo) de la Dirección General de Tecnologías e Innovación Digital".

RETIRADA DE MATERIALES PROPIEDAD DE LA EMPRESA

- La retirada de materiales propiedad de la empresa, considera en su control que los equipos, información o el software, no deben sacarse de las instalaciones sin autorización previa de Dirección General de Tecnologías e Innovación Digital Dirección General de Tecnologías e Innovación Digital.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

El personal de la Dirección General de Tecnologías e Innovación Digital, debe ser responsables de la administración y cumplimiento de la presente política, así como de la aplicación de los criterios necesarios para preservar los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC´s deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, de reglamentos, jurídicos, financieros o de cualquier otra índole incluyendo los avances tecnológicos que tengan impacto en las facultades del área de Recursos Humanos, la Dirección de Administración y la Dirección de Servicios Tecnológicos.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad***.

Los servicios de auditoría al Sistema de Gestión de la Seguridad de la Información (SGSI), o a cualquier otro elemento de gestión de tecnología deberá ser efectuado por entidades externas a para las Dependencias y Entidades del Estado por lo menos una vez al año.

4.0 Sanciones y Observaciones

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Recursos Humanos	El área administrativa facultada para autorizar cualquier movimiento laboral del personal del uso y aprovechamiento de Tecnologías de la Información
Usuario	Persona que utiliza los sistemas informáticos de la DGTID al que se le ha proporcionado una "Cuenta de usuario asociada a una contraseña", siendo estos administrados por el Directorio Activo de la DGTID. Por lo que en el APE no existe la figura de "Usuario" que no tenga acceso al uso de internet o correo electrónico.
Infraestructura tecnológica	Sistemas de información, servicios de información, software, programas, rutinas, dispositivos, sistemas de comunicaciones, sistemas de transmisión de voz y/o datos y cualquier otro medio eléctrico, electrónico o impreso propiedad de la DGTID
Propiedad	Cualquier tipo de hardware o software que el uso y aprovechamiento de Tecnologías de la Información tenga en propiedad, copropiedad, arrendamiento, subarrendamiento, préstamo, donación o cualquier otra forma en que el goce de los derechos esté a favor de la DGTID
UPS	Unidad de Energía Interrumpible

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID.*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

GESTIÓN DE COMUNICACIONES Y OPERACIONES

RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN

SEGREGACIÓN DE FUNCIONES

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones A.10.1 Responsabilidades y procedimientos de operación.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión concluido***
A.10.1 A.10.1.3	Responsabilidades y procedimientos de operación Segregación de Tareas	2	2.0	Concluido
Vigencia a partir de:		**Marzo 2019**		

Título de la política

Segregación de funciones.

Objetivo

Delimitar las funciones del personal de la DGTID, con la finalidad de evitar riesgos innecesarios, conflictos de intereses, mal uso accidental o deliberado de los activos de información del Estado de Oaxaca.

1.0 Propósito

Garantizar que la DGTID cuente con la adecuada separación de funciones para reducir el riesgo de mal uso, accidental o deliberado del sistema, considerando la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir las oportunidades de modificación no autorizada o mal uso de la información o los servicios.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para todas las áreas que conforman la DGTID.

3.0 Política

3.1 Descripción de Política

- Deberá realizarse la separación de las funciones de las áreas que conforman la DGTID, sobre todo de aquellas que desarrollen sistemas y aplicaciones, con la finalidad de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

- Deberá asegurarse la independencia de las funciones de auditoría de seguridad, tomando precauciones para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

    - Separar actividades que requieren complicidad para defraudar.
    - Diseñar controles, si existe peligro de contubernio, de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

- Deberá asegurarse que un individuo no pueda llevar a cabo todas las fases de una operación/transacción, desde su autorización, pasando por la custodia de activos y el mantenimiento de los registros maestros necesarios.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente a la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

La Dirección General de Tecnologías e Innovación Digital, debe ser responsable de la administración y cumplimiento de la presente política, así como de la aplicación de los criterios necesarios para preservar los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, modificación de funciones, de reglamentos, jurídicos, financieros o de cualquier otra índole incluyendo los avances tecnológicos que tengan impacto en las facultades del área de Recursos Humanos, la Dirección de Administración y la Dirección de Servicios Tecnológicos.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.
Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad***.

Los servicios de auditoría al Sistema de Gestión de la Seguridad de la Información (SGSI), o a cualquier otro elemento de gestión de tecnología deberá ser efectuado por entidades externas a para las Dependencias y Entidades del Estado por lo menos una vez al año.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Segregación de Funciones	Separación y delimitación de tareas, funciones, deberes.
Complicidad	Confabulación, unirse a otra persona con un fin común.
Riesgo	Vulnerabilidad ante un posible daño. Peligro.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

SEPARACIÓN DE LOS RECURSOS DE DESARROLLO, PRUEBA Y OPERACIÓN

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones A.10.1 Responsabilidades y procedimientos de operación.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión concluido***
A.10.1 A.10.1.4	Responsabilidad y procedimientos de operación Separación de los recursos de desarrollo, prueba y operación	2	2.0	Concluido
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Separación de los recursos de desarrollo, prueba y operación.

Objetivo

Separar los recursos y los ambientes de desarrollo con el fin de tener un entorno seguro donde la exposición al riesgo se reduzca.

1.0 Propósito

Garantizar que los desarrollos y diseños de solución tecnológica que ejecute de la *Dirección General de Tecnologías e Innovación Digital* cuente con una separación entre la producción y el desarrollo de sistemas con el fin de lograr un entorno informático seguro, evitando así, que los desarrolladores, usuarios y otros puedan realizar modificaciones al software de producción. De esta forma se reduce considerablemente la variedad de exposiciones a riesgos.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para las áreas de desarrollo de sistemas de la Dirección de Servicios Tecnológicos de la *Dirección General de Tecnologías e Innovación Digital*.

3.0 Política

3.1 Descripción de Política

- Los ambientes de desarrollo, prueba y operación estarán separados preferentemente en forma física y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

- Se deberá ejecutar el software de desarrollo y de operación, en diferentes ambientes de operaciones, equipos, directorios o librerías, así como también separar las actividades de desarrollo y prueba, en entornos diferentes y por medio de estrictos controles de acceso.

- No permitir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento de este.

- Se deberán utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Se les prohíbe a los usuarios compartir contraseñas en estos sistemas.

- Las interfaces de los sistemas deberán identificar claramente a qué instancia se está realizando la conexión.

- Se deberá aplicar la política de clasificación de información y su estándar, para establecer a los propietarios de la información para cada uno de los ambientes de procesamiento existentes.

- El personal de desarrollo no tendrá acceso al ambiente de operaciones. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

- El software de aplicaciones de producción en etapa de desarrollo debe permanecer estrictamente separado de este mismo tipo de software en período de prueba, a través de sistemas informáticos físicamente separados o directorios o bibliotecas separadas con estrictos controles de acceso.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- El desarrollo y mantenimiento del código fuente de las aplicaciones de producción; el período de prueba y operación de las aplicaciones de producción; y el manejo de los datos de las aplicaciones de producción, deben ser realizadas por distintas personas de acuerdo con la política de **Segregación de funciones**, de tal forma que se eviten riesgos innecesarios.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

La Jefatura de la Unidad de Planeación y Control de TIC's, personal de la Dirección de Servicios Tecnológicos y cada una de las Jefaturas de la DGTID, deben ser responsables de la administración y cumplimiento de la presente política, así como de la aplicación de los criterios necesarios para preservar los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC´s , deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política, así como a las actualizaciones pertinentes derivadas de los cambios laborales, modificación de funciones, de reglamentos, jurídicos, financieros o de cualquier otra índole incluyendo los avances tecnológicos que tengan impacto en las facultades del área de Recursos Humanos, la Dirección de Administración y la Dirección de Servicios Tecnológicos.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Las auditorías o revisiones serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.
Todos los esfuerzos de los procesos de auditorías o revisiones se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información, así como la preservación de las características principales de la información: ***disponibilidad, integridad y confidencialidad***.

Los servicios de auditoría al Sistema de Gestión de la Seguridad de la Información (SGSI), o a cualquier otro elemento de gestión de tecnología deberá ser efectuado por entidades externas por lo menos una vez al año.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Ambiente de Desarrollo	Lugar en donde se almacena el software y aplicaciones que se utiliza para el desarrollo
Ambiente de prueba	Lugar en donde se efectúan las pruebas al software desarrollado. Debe pasar por este período de pruebas antes de ser liberado al ambiente de producción
Ambiente de operaciones	Se refiere al ambiente de producción
Período de prueba	Se refiere a los pasos por los que debe pasar un programa de aplicaciones previo a ser utilizado en un ambiente de producción.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones históricas de la política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA

GESTIÓN DE CAPACIDADES

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones A.10.3 Planificación y aceptación del sistema.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.10.3 A.10.3.1	Planificación y aceptación del sistema Gestión de Capacidades	2	2.0	En proceso
Vigencia a partir de:	**Marzo 2019**			

Título de la política

Gestión de Capacidad de la Infraestructura Tecnológica.

Objetivo

Efectuar el monitoreo de la gestión de la capacidad de los sistemas en operación e infraestructura tecnológica y proyectar las futuras demandas de operación procesamiento, transaccionalidad, comunicación y almacenamiento.

1.0 propósito

Garantizar que los sistemas e información del Estado cuenten con un procesamiento y almacenamiento de información adecuados, mediante el monitoreo de las necesidades de capacidad de los sistemas en operación y la proyección de las futuras demandas.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación:

El ámbito de aplicación de la presente política se establece para todas la infraestructura en administración y custodia de la DGTID.

3.0 Política

3.1 Descripción de Política

- La Dirección de Servicios Tecnológicos, efectuará el procedimiento de Gestión de la Capacidad, englobando los tres procesos:

  Gestión de la capacidad de negocio,
  Gestión de la capacidad del servicio,
  Gestión de la capacidad de los recursos.

- La Dirección General de Tecnologías e Innovación Digital, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectará mediante planes de capacidad asociados a los niveles de servicio acordados, las futuras demandas, a fin de garantizar un procesamiento y almacenamiento de información adecuados.

- La Dirección General de Tecnologías e Innovación Digital, deberá considerar los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información para el período estipulado de vida útil de cada componente.

- La Dirección General de Tecnologías e Innovación Digital, deberá controlar el rendimiento de la infraestructura de TI, así como gestionar y racionalizar la demanda de servicios de TI.

- La Dirección de Servicios Tecnológicos, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y así estar en posibilidades de planificar una adecuada acción correctiva.

- La Dirección General de Tecnologías e Innovación Digital, mediante la Gestión de Capacidades, gestionará el aprovechamiento adecuado de los recursos a fin de no realizar inversiones innecesarias que acarreen gastos adicionales de mantenimiento y

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

administración, o bien recursos insuficientes con la consecuente degradación de la calidad del servicio.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

El personal de cada una de las Jefaturas de la Dirección General de Tecnologías e Innovación Digital, deben ser responsables de la administración y cumplimiento de la presente política, así como de la aplicación de los criterios necesarios para preservar los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Gestión de la capacidad de negocio	Centra su objeto de atención en las necesidades futuras de usuarios y usuarios.
Gestión de la capacidad del servicio	Analiza el rendimiento de los servicios TI con el objetivo de garantizar los niveles de servicio acordados
Gestión de la capacidad de los recursos	Estudia tanto el uso de la infraestructura TI como sus tendencias para asegurar que se dispone de los recursos suficientes y que estos se utilizan eficazmente.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza *L.I. Eduardo José Herrerías López* *Director General* *Dirección General de Tecnologías e Innovación Digital*	Revisa *Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

ACEPTACIÓN DEL SISTEMA

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones A.10.3 Planificación y aceptación del sistema.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en sistema, concluido***
A.10.3 A.10.3.2	Planificación y Aceptación del Sistema Aceptación del Sistema	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Aceptación del Sistema, Liberación y Puesta en producción.

Objetivo

Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

1.0 Propósito

Garantizar que los sistemas desarrollados por la DGTID, previos a ser liberados para las áreas de negocio, hayan sido sometidos a una serie de pruebas exhaustivas antes de estar considerados para estar en el ambiente de operaciones.

2.0 Ámbito de Aplicación

El ámbito de aplicación de la presente política se establece para todas las áreas de operación y de negocio que solicitan desarrollos, o nuevos sistemas a la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.0 Política

3.1 Descripción de Política

- La Dirección General de Tecnologías e Innovación Digital, deberá efectuar pruebas exhaustivas a los sistemas, actualizaciones y nuevas versiones, desde la etapa de desarrollo de estos hasta su aceptación formal. Dichas pruebas deberán estar documentadas y aprobadas, antes de que dichos sistemas sean migrados al ambiente de producción.

- La Dirección General de Tecnologías e Innovación Digital y las áreas usuarias deberán estar en contacto directo a fin de que los sistemas liberados cumplan las expectativas de ambas partes, se lleven a cabo las pruebas apropiadas y se confirme que se ha cumplido totalmente con el criterio de aceptación.

- La Dirección General de Tecnologías e Innovación Digital, verificará el impacto en el desempeño y los requerimientos de capacidad de los equipos de cómputo.

- La Dirección de Servicios Tecnológicos, deberá garantizar la recuperación ante errores, reinicio y planes de contingencia.

- La Dirección de Servicios Tecnológicos, deberá implementar los controles de seguridad necesarios para los sistemas que libere, así como asegurarse que la instalación del nuevo sistema no afectará negativamente al resto de los sistemas existentes, especialmente en los períodos de alto grado de procesamiento.

- La Dirección General de Tecnologías e Innovación Digital, deberá establecer programas de capacitación y de entrenamiento en la operación y/o uso de nuevos sistemas.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

El personal de la Dirección de Servicios Tecnológicos y las áreas usuarias de la DGTID, deben ser responsables de la administración y cumplimiento de la presente política, así como de la aplicación de los criterios necesarios para preservar los sistemas de información y la infraestructura tecnológica de para las Dependencias y Entidades del Estado.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar una revisión y seguimiento permanente al cumplimiento de la presente política.

3.4 Revisiones y Auditorías

Las auditorías o revisiones serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información por lo menos una vez al año.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

5.0 Definición de Términos

Término	*Definición*
Pruebas exhaustivas	Pruebas muy completas que no dejen lugar a dudas y donde se detecten los posibles errores.
Áreas usuarias	Toda aquella área de la DGTID que haga uso de los sistemas y de los servicios de TI.
Migración	Traspaso de la información a un ambiente diferente.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y DESCARGABLE

PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones. A.10.4 Protección contra código malicioso y descargable.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.10.4 A.10.4.1	Protección contra código malicioso y descargable Controles contra el código malicioso	2	2.0	En proceso
Vigencia a partir de:	**Marzo 2019**			

Título de la Política

Política de protección contra código malicioso.

Objetivo

Establecer las condiciones para la prevención de incidentes por uso de código malicioso o Programa maligno en los sistemas bajo la administración y custodia de la DGTID.

1.0 Propósito

Establecer los requisitos que se deben implementar en todas las computadoras conectadas a las redes y las acciones para evitar ataques por código malicioso, definiendo acciones para la detección, prevención y eliminación eficaz y oportuna de cualquier tipo de virus informáticos, así como la actualización permanente y oportuna de los sistemas antivirus instalados.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica para todas las computadoras y servidores, en administración y custodia de la DGTID, aplica a proveedores, usuarios o externos que deban tener acceso a los sistemas de información o servicios de información de la DGTID

En el caso de los servidores de archivos, servicios /ftp/tftp/proxy, servicios de bases de datos, páginas Web, Active Directory, servicios DNS, servicios DHCP y cualquier equipo con capacidad de transmitir o recibir información deben tener mecanismos para la detección y eliminación oportuna de cualquier tipo de virus informático.

3.0 Política

3.1 Descripción de la Política

- Todas las computadoras propiedad de las Dependencias de la APE, o que se conectan con la red o redes del Estado, deben cumplir con los estándares y el software y la instalación de antivirus.

- En el caso de que existan computadoras o equipos infectadas o vulnerados, estos se deben desconectarse de inmediato de la red hasta que se puedan clasificar como computadoras libres de virus libres de intervención. Deberá ejecutarse el proceso establecido de Gestión de Incidentes.

- Queda prohibido el uso de software no licenciado o autorizado por la Dirección de Servicios Tecnológicos.

Con el objeto de garantizar la operación óptima de los servidores específicamente, el o los administradores de servidores y personal de soporte técnico, deben ejecutar las siguientes acciones básicas de protección de virus y que no se limitan a:

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Computadoras

- La Jefatura de Departamentos de Infraestructura debe gestionar la adquisición del o los paquetes de aplicaciones antivirus más actualizados posibles para su instalación los equipos de cómputo propiedad de la DGTID

- La Jefatura de Departamentos de Infraestructura debe realizar la instalación y configuración de las aplicaciones antivirus para su operación, en todos y cada uno de los equipos de cómputo propiedad del Estado de Oaxaca.

- La Jefatura de Departamentos de Infraestructura debe configurar el software antivirus para que efectúe la revisión del equipo al menos una vez por semana.

- La Jefatura de Departamentos de Infraestructura debe configurar el software antivirus para que ejecute el proceso de actualización de la base de datos de antivirus diariamente o cuando existan modificaciones a la base de datos por parte del fabricante del software.

- La Jefatura de Departamentos de Infraestructura debe poner en cuarentena o eliminar totalmente todos y cada uno de los archivos marcados como infectados en las computadoras infectadas que los antivirus no puedan reparar y que no representen pérdida o daño al funcionamiento del o los sistemas o servicios instalados.

- La Jefatura de Departamentos de Infraestructura desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. Dichos controles deberán abarcar entre otros:

    - Prohibir el uso de software no autorizado por la DGTID
    - Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
    - Concienciar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos. Instruir al usuario de que en el caso de que sospeche de la existencia de un virus en su equipo, deberá desconectarse de la conexión de red, apagarlo inmediatamente y comunicarse con la mesa de servicio. En ningún caso deberá intentar eliminarlo él mismo.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Servidores

- La Jefatura de Departamentos de Infraestructura deberá gestionar la adquisición del o los paquetes de aplicaciones antivirus más actualizados posibles para su instalación en el o los servidores.

- La Jefatura de Departamentos de Infraestructura deberá realizar la instalación y configuración de las aplicaciones antivirus para su operación en el o los servidores.

- La Jefatura de Departamentos de Infraestructura deberá ejecutar al menos una vez por semana, el proceso de rastreo y eliminación de virus de cada servidor.

- La Jefatura de Departamentos de Infraestructura deberá realizar la actualización de las aplicaciones de antivirus en cada uno de los servidores.

- La Jefatura de Departamentos de Infraestructura podrá y deberá poner en cuarentena o eliminar totalmente todos y cada uno de los archivos marcados como infectados y que los antivirus no puedan reparar y que no representen pérdida o daño al funcionamiento del o los sistemas o servicios instalados.

- Cualquier actividad con la intención de crear y/o de distribuir programas perjudiciales dentro de las redes de comunicaciones del uso y aprovechamiento de Tecnologías de la Información (ejemplo: virus, gusanos, caballos de Troya, bombas del correo electrónico, etc.) están prohibidos totalmente de acuerdo con la *Política de uso Aceptable.*

- En caso de requerir información adicional sobre virus y métodos de detección o remoción de virus, se debe consultar el sitio del fabricante del software autorizado por el uso y aprovechamiento de Tecnologías de la Información.

Excepciones conocidas: Las máquinas con los sistemas operativos diferentes a los productos de Microsoft, se exceptúan al momento de la elaboración y publicación de esta política. Sin embargo, es obligatorio que los administradores de cada plataforma distinta a los productos servidores de Microsoft, destinen tiempo y recursos al monitoreo de virus y software perjudicial para cada una de las plataformas que administran. En caso de reportarse código perjudicial conocido y documentado, tomen las acciones preventivas necesarias y registren estos hechos y las medidas en las bitácoras o medios asignados para tal efecto.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, de la Dirección de Servicios Tecnológicos deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

3.4 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por Dirección General de Tecnologías e Innovación Digital y personal de la DGTID

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Virus informático	Programa, rutina o software creado para causar daño a la información contenida en equipos o dispositivos de cómputo. Se considera virus a cualquier software, código o programa que se instale, analice, modifique o transmita información sin consentimiento explícito del usuario.
Antivirus	Programa dedicado a detectar en una computadora la existencia de virus, eliminarlos en caso de encontrarlos o en su defecto a marcarlos como código de contenido peligroso.
Código perjudicial o malicioso	Cualquier programa, subprograma, rutina, subrutina, aplicación, algoritmo o código ejecutable o interpretado que permita llevar a cabo acciones para la pérdida, alteración o transmisión no autorizada de datos y/o información. Programa o archivo, que es dañino para la computadora, está diseñado para insertar virus, gusanos, troyanos o spyware intentando conseguir algún objetivo, como podría ser el de recabar información sobre el usuario o sobre la computadora en sí.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

GESTIÓN DE SEGURIDAD DE LAS REDES

POLÍTICA DE TELECOMUNICACIONES

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones. A.10.6. Gestión de la Seguridad de las Redes.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.10.6 A.10.6.1 A.10.6.2	Gestión de la Seguridad de las Redes Controles de red. Seguridad de los servicios de red	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Política de Telecomunicaciones y Red de Servicios

Objetivo

Asegurar la protección de la información en todas las redes y plataforma de servicios de telecomunicaciones en administración y custodia de la DGTID, así como la protección de la infraestructura y soporte.

1.0 Propósito

Minimizar los efectos de posibles interrupciones en los servicios de red y dispositivos de Seguridad Perimetral, así como el acceso no controlado a los sistemas de información de la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica para todas las redes, servicios y dispositivos de seguridad perimetral, tanto si estos servicios se prestan dentro de la DGTID o son subcontratados. Esta política deberá ser atendida por los terceros que procesen información de la DGTID.

Propiedad

Todas las Redes de servicios y sus respectivos segmentos administradas por la DGTID deben tener asignado un dueño.

3.0 Política

3.1 Descripción de la Política

Transferencia de Información

- Se debe proteger la integridad y confidencialidad de la información clasificada como reservada y confidencial, cuando sea transferida dentro de la red de la DGTID o hacia redes externas.

- El tráfico y acceso hacia la red interna debe estar restringido y protegido para prevenir afectación a la ***integridad, confidencialidad y disponibilidad*** de la información de la Dirección General de Tecnologías e Innovación Digital y la Tecnología de la Información que la soporta.

- Se debe realizar un Análisis de Riesgos para determinar los controles que se deben implementar entre la red interna y la red externa, así como entre segmentos de red (Ej. Firewalls y Sistema de Detección de Intrusos).

Componentes

- Los dispositivos de Telecomunicaciones (ruteadores, switches, hubs y conmutadores), así como los dispositivos de Seguridad Perimetral (Ej. Firewall y sistema de detección de intrusos) deben ser administrados y configurados de acuerdo a los lineamientos estándar, que contemplen controles para restringir el acceso a los dispositivos y controles para proteger la integridad y disponibilidad de los dispositivos. El sistema operativo debe estar configurado para ser seguro antes de ser utilizado en producción.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Los dispositivos de Telecomunicaciones y Seguridad Perimetral deben estar resguardados en un área segura que cumpla con los requerimientos de control de acceso y control ambiental especificados en la Política de Seguridad Física.

Identificación de Componentes y Conexiones

- La Dirección General de Tecnologías e Innovación Digital debe mantener un diagrama de red actualizado en el cual se identifiquen todos los puntos de acceso a la red, conexiones externas, segmentos de red y componentes de Telecomunicaciones y de Seguridad Perimetral.

Administración de Direcciones IP

- La Dirección General de Tecnologías e Innovación Digital, debe mantener un adecuado control y administración de las direcciones IP´s. Se deben implementar controles para prevenir la clonación de direcciones IP´s.
- La red interna debe estar segmentada para dividir grupos de servicios, usuarios o sistemas, para proteger la información confidencial.
- Se debe utilizar traducción de direcciones IP´s (NAT) para proteger las direcciones IP´s internas.

Autorización de Conexiones

- Las conexiones externas a la red interna de la Dirección General de Tecnologías e Innovación Digital deben estar autorizadas por esta Dirección.
- Por lo menos cada seis meses la Dirección General de Tecnologías e Innovación Digital debe realizar una revisión de las conexiones externas para evaluar su continuo requerimiento.

Internet

- La Dirección de Servicios Tecnológicos, debe monitorear el uso de Internet y bloquear el acceso a páginas con contenido de entretenimiento u ofensivo (sexual, sexista, racista, violento u otro contenido ofensivo).

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Cableado

- El cableado de Telecomunicaciones debe estar protegido contra interferencia o daño físico, de acuerdo a los requerimientos especificados en la Política de Seguridad Física.

Segmentación de Redes

- La arquitectura de red de la Dirección General de Tecnologías e Innovación Digital debe estar segmentada aplicando los niveles de seguridad que se requieran en cada uno de los segmentos. La separación debe realizarse de acuerdo al tipo de información que se envía o transmite.

- Se debe considerar limitar la comunicación por puertos.

- Un equipo conectado a la red no debe representar un puente inseguro entre dos o más redes.

- Se deben implementar controles de integridad y confidencialidad para prevenir la intercepción o modificación de los datos mientras estos son transmitidos por la red.

- Cualquier tipo de extensión, expansión, enlace o conexión con redes públicas o externas al APE deberá contar con un análisis de riesgos e impacto para determinar el nivel de seguridad requerido, habiéndose tomado medidas de acción temprana.

Redes Inalámbricas

- El uso de la red inalámbrica debe estar restringido y justificado de acuerdo a las necesidades de la organización. Se debe realizar un análisis de riesgos para determinar la viabilidad del uso de redes inalámbricas. En caso de que se determine utilizar redes inalámbricas se debe considerar lo siguiente:
    - Uso de clave de red y cifrado de datos.
    - Los dispositivos de la red inalámbrica deben estar protegidos para evitar su robo.
    - Se debe mantener actualizado un diagrama de ubicación de los dispositivos.
    - Se debe realizar una revisión periódica en los diferentes pisos de las instalaciones de APE, para identificar redes inalámbricas no autorizadas.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Se debe considerar a la red inalámbrica como no confiable, por lo que se deben implementar controles entre la red inalámbrica y alámbrica para prevenir accesos no autorizados. Estos controles deben incluir como mínimo:

  - Firewall y sistema de detección de intrusos.
  - Ubicación de antenas lejos de ventanas y paredes que den hacia la calle.
  - Restricción de dispositivos que se conectan a la red alámbrica.

Conmutador

- Entre los controles a implementar deben estar contemplados:

  - Analizar las funciones que son requeridas y deshabilitar las no requeridas.
  - Cambiar las contraseñas predefinidas por el fabricante.
  - Controlar el acceso de llamadas a larga distancia y celular.
  - Bloquear las llamadas a números con cargo (01900).
  - Definir permisos de acceso para el personal de administración y mantenimiento según las funciones realizadas.
  - Bloquear las cuentas por inactividad.
  - Antes de instalar nuevas versiones o parches, verificar la integridad y origen de los archivos.
  - Configurar la generación de registros de llamadas (logs).

Análisis de Vulnerabilidades y Pruebas de Penetración

- Por lo menos cada 6 meses se debe realizar un análisis de vulnerabilidades de la red interna y del equipo de telefonía. Así mismo se debe generar un reporte con las vulnerabilidades detectadas, recomendaciones de mejora y un programa de trabajo con acciones correctivas y fechas compromiso.

- Por lo menos una vez al año se debe realizar una prueba de penetración por un especialista para evaluar la efectividad de las medidas de control implementadas contra ataques internos y externos.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Se debe firmar un acuerdo de confidencialidad, así como definir y documentar el objetivo, alcance y restricciones de las pruebas. Se debe generar un reporte ejecutivo y un reporte detallado, los cuales incluyan como mínimo:

    - Descripción de la prueba (Objetivo, Alcance y Restricciones).
    - Resumen del impacto a la organización por las vulnerabilidades encontradas.
    - Metodología utilizada.
    - Métodos de prueba y herramientas utilizadas.
    - Listado de activos tecnológicos probados.
    - Huecos de seguridad identificados por activo, ordenados por nivel de riesgo.
    - Causa de las debilidades encontradas.
    - Posibles consecuencias de las vulnerabilidades encontradas.
    - Recomendaciones de mejora.
    - Conclusiones.
    - Anexo con reportes generados por las herramientas utilizadas.

- La Dirección General de Tecnologías e Innovación Digital debe generar un programa de trabajo con acciones correctivas y fechas compromiso.

- Es responsabilidad del Oficial de Seguridad de la Información, coordinar los análisis de vulnerabilidades y las pruebas de penetración.

Mantenimiento de Hardware y Software

- Periódicamente se debe realizar mantenimiento preventivo para garantizar la disponibilidad de los dispositivos de Telecomunicaciones y Seguridad Perimetral.

- La Dirección General de Tecnologías e Innovación Digital debe elaborar un calendario de mantenimiento preventivo y generar una bitácora de registro de actividades de mantenimiento (preventivo y correctivo).

- Periódicamente se debe realizar actualización de versiones y parches de Sistemas Operativos.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Control de Cambios

- Se debe llevar un registro y control de los cambios realizados a los dispositivos de Telecomunicaciones y Seguridad Perimetral.

- Se debe realizar un análisis de impacto de los cambios a realizar.

- Los cambios deben estar aprobados por el dueño antes de su construcción y autorizados por el mismo dueño antes de su liberación a producción. Los cambios mayores o de alto impacto deben estar autorizados además por el Oficial de Seguridad de la Información.

- Se deben realizar pruebas antes de implementar los cambios en producción.

Planeación de Capacidad y Monitoreo de Fallas

- El personal encargado de la administración de las Telecomunicaciones debe monitorear y reportar el uso de este servicio, para identificar requerimientos de crecimiento. Se debe llevar una bitácora o reporte de monitoreo de uso. Este personal se debe coordinar con el Administrador de la Red para planear su optimización y garantizar su continua disponibilidad.

- El personal encargado de la administración de las Telecomunicaciones debe llevar un registro de las fallas y problemas presentados.

Memorias Técnicas

- El personal encargado de la administración de las Telecomunicaciones y dispositivos de Seguridad Perimetral debe mantener su documentación actualizada sobre la configuración de los dispositivos.

Registros de Auditoria

- Los dispositivos de Telecomunicaciones y Seguridad Perimetral deben estar configurados para generar registros de auditoría (logs). Dichos registros deben estar

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

protegidos de manera que no puedan ser modificados. La depuración de dichos archivos debe estar restringida a personal de monitoreo de Seguridad de la Información. Los registros de auditoría deberán ser resguardados en línea por un mes y fuera de línea por un año.

- Estos registros deben ser monitoreados de acuerdo a lo definido en la Política de Monitoreo.

Sincronización

- Todos los servidores y equipos de comunicaciones deben estar exactamente sincronizados en sus respectivos relojes, con el objeto de asegurar la precisión de registros de auditoría.

Respaldos

- La Dirección General de Tecnologías e Innovación Digital es responsable de respaldar y restaurar la configuración de los dispositivos de Telecomunicaciones y Seguridad Perimetral, de acuerdo a los requerimientos definidos en el estándar de respaldos.

Protección de Documentación

- Los manuales, guías de configuración y memorias técnicas de los activos de Tecnología de la Información deben estar resguardados en un área segura. El acceso a dicha documentación debe estar controlado.

Personal

- La Dirección de Servicios Tecnológicos debe verificar y garantizar que se cuente con personal especializado y capacitado para desempeñar las funciones de administración de Telecomunicaciones y dispositivos de Seguridad Perimetral.

- Deberá efectuarse un análisis de riesgos que identifique:
    - Activo

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Vulnerabilidades
- Amenazas
- Probabilidad de ocurrencia de las amenazas
- Impacto estimado
- Regulaciones que deben cumplirse

- La administración de riesgos deberá llevarse a cabo en forma periódica.

- La Administración de riesgos deberá evaluar y administrar los riesgos, asumiendo que toda la Organización debe estar consciente que siempre existen riesgos residuales con los que tiene que llevarse a cabo el trabajo, de tal forma que el impacto que conlleven sea el menor posible.

- Con la finalidad de garantizar el mínimo nivel de riesgo, se deberá concientizar al personal sobre la necesidad de cumplir y respetar las políticas de seguridad de la información y los estándares, mismos que pretenden prever el sabotaje, el terrorismo, el fraude, los errores y las omisiones, las interrupciones del servicio, el robo de equipos y la violación de la privacidad, entre otros, cubriendo las necesidades de la Dirección General de Tecnologías e Innovación Digital en materia de seguridad.
- Todos los sistemas en producción deberán ser evaluados periódicamente por la Dirección General de Tecnologías e Innovación Digital, para determinar el mínimo conjunto de controles requeridos para reducir y mantener los riesgos a un nivel aceptable de tal forma que puedan ser priorizados por riesgo.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.3 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por el uso y aprovechamiento de Tecnologías de la Información o personal de la DGTID

Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Virus informático	Programa, rutina o software creado para causar daño a la información contenida en equipos o dispositivos de cómputo. Se considera virus a cualquier software, código o programa que se instale, analice, modifique o transmita información sin consentimiento explícito del usuario.
Antivirus	Programa dedicado a detectar en una computadora la existencia de virus, eliminarlos en caso de encontrarlos o en su defecto a marcarlos como código de contenido peligroso.
Código perjudicial o malicioso	Cualquier programa, subprograma, rutina, subrutina, aplicación, algoritmo o código ejecutable o interpretado que permita llevar a cabo acciones para la pérdida, alteración o transmisión no autorizada de datos y/o información. Programa o archivo, que es dañino para la

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Término	*Definición*
	computadora, está diseñado para insertar virus, gusanos, troyanos o spyware intentando conseguir algún objetivo, como podría ser el de recabar información sobre el usuario o sobre la computadora en sí.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

MANIPULACIÓN DE LOS SOPORTES

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones. A.10.7 Manipulación de los Soportes.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión concluido***
A.10.7 A.10.7.1 A.10.7.2	Manipulación de los Soportes Gestión de soportes extraíbles Retirada de soportes	0	0	Programada
Vigencia a partir de:	**Marzo 2019**			

Título de la Política

Manipulación de los soportes

Objetivo

Establecer las condiciones de uso y controles para reducir los riesgos de incidentes de seguridad en la manipulación, gestión y retirada de soportes.

1.0 Propósito

Establecer las condiciones de uso, aprovechamiento, alcances y controles para reducir los riesgos de incidentes de seguridad en la manipulación de los soportes, a fin de prevenir daños y proteger la información que se maneja o almacena en ellos.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica para todos los soportes extraíbles utilizados por empleados y usuarios o externos que deban tener acceso a los sistemas de información o servicios de información del Estado.

3.0 Política

3.1 Descripción de la Política

GESTIÓN DE SOPORTES EXTRAÍBLES

- La Dirección General de Tecnologías e Innovación Digital, por conducto de la Jefatura de Departamento de Soporte Técnico y Telecomunicaciones, será la responsable de llevar a cabo la administración de los soportes extraíbles/removibles, tales como: cintas, discos, memorias flash, etc.

- Se deberán establecer los controles pertinentes para que los soportes, en el caso de ser reutilizables, cuenten con las medidas de seguridad mínimas indispensables que la Jefatura de Departamento de Soporte Técnico y Telecomunicaciones, considere necesarias.

RETIRADA DE SOPORTES

- La Jefatura de Departamento de Soporte Técnico y Telecomunicaciones, mantendrá el registro de los soportes extraíbles que sea necesario retirar de las instalaciones de la Dirección de Servicios Tecnológicos y del propio APE para su instalación en alguna otra cede; por lo antes indicado durante el transporte fuera de los límites físicos de la Dirección General de Tecnologías e Innovación Digital los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

- Deberá asegurarse de que dichos soportes hayan sido revisados de tal forma que no sea retirada información confidencial, a menos, que dicha información cuente con la autorización requerida para su retirada en dichos soportes.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Monitoreo

Se deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

3.4 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por Dirección General de Tecnologías e Innovación Digital o personal del uso y aprovechamiento de Tecnologías de la Información

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

5.0 Definición de Términos

Término	***Definición***
Soportes Extraíbles	Aquellos complementos que tienen la capacidad de almacenar información y que tiene la característica de ser portables con mayor facilidad debido a su tamaño.
Disposición Pública	Que se encuentre disponible para consulta de cualquier persona.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

INTERCAMBIO DE INFORMACIÓN

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones. A.10.8 Intercambio de Información.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión concluido***
A.10.8 A.10.8.2 A.10.8.4	Intercambio de Información Acuerdos de intercambio Mensajería electrónica	2	2.0	En proceso
Vigencia a partir de:	**Marzo 2019**			

Título de la Política

Seguridad en el intercambio de información.

Objetivo

Establecer las condiciones de uso y controles para reducir los riesgos de incidentes de seguridad en el intercambio de información.

1.0 Propósito

Establecer las condiciones de uso, aprovechamiento, alcances y controles para reducir los riesgos de incidentes de seguridad en el intercambio de información, a fin de prevenir daños y proteger la información que se maneja e intercambia.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica para todas las computadoras y servidores, tanto los arrendados o propiedad de la DGTID, instalados y en operación tanto en las instalaciones de la APE como de otras instalaciones externas a las que se tenga acceso, utilizados por empleados del Estado de Oaxaca, proveedores, usuarios o externos que deban tener acceso a los sistemas de información o servicios de información que administre o custodie la DGTID.

3.0 Política

3.1 Descripción de la Política

ACUERDOS DE INTERCAMBIO

- El software desarrollado por unidades de desarrollo de la APE, debe ser distribuido sólo en la forma de código objeto.

- Los intercambios de software o información interna entre la DGTID y los terceros deben estar acompañados por un acuerdo escrito que especifique los términos del intercambio y la manera en que el software o la información se manejará y protegerá.

- Deberá utilizarse el **Estándar de clasificación de información**, para la identificación de la información, garantizando que la información sea adecuadamente protegida.

CORREO ELECTRÓNICO

- El correo electrónico institucional de la DGTID es una herramienta de trabajo, comunicación e intercambio de información, por ende, solo es posible realizar actividades que estén relacionadas con los propósitos y funciones institucionales de operación. Debe ser utilizado de manera racional, evitando su abuso, derroche o desaprovechamiento.
  Debido a que el correo institucional es una herramienta de trabajo, la Dirección de Servicios Tecnológicos, tiene el derecho de efectuar el monitoreo de este.

- El uso indebido del servicio de correo electrónico será motivo de suspensión temporal de la cuenta de correo del usuario o de acuerdo a la gravedad la eliminación de la misma.

- El usuario será responsable de la información que sea enviada con su cuenta.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- La Dirección de Servicios Tecnológicos, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional. Podrá cancelar o inhabilitar la cuenta de cualquier usuario sin previo aviso, si se considera que el usuario ha contravenido los lineamientos aquí mencionados.

- El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor. Los usuarios son responsables de su información y, por ende, deben guardar regularmente la que consideren de importancia.

- Queda estrictamente prohibida la difusión de contenidos inadecuados y/o masivos, tales como: complicidad con hechos delictivos, apología del terrorismo, uso y/o distribución de programas piratas, mensajes difamatorios, hostigantes o de naturaleza explícitamente sexual u ofensiva a persona alguna sobre la base de raza, sexo, origen, orientación sexual, religión, creencias políticas o discapacidad física, publicidad "spam", todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento piramidal, cadenas, virus o código malicioso en general.

- Los usuarios del correo electrónico no deberán emplear sus firmas autógrafas digitalizadas con el fin de dar la impresión de que un mensaje de correo electrónico u otra comunicación electrónica ha sido firmada por el remitente.

- El tamaño máximo para archivos adjuntos no deberá exceder de los 10 MB por mensaje y la cantidad máxima de destinatarios por mensaje será de 50, esta cantidad incluye los campos CC (con copia) y CCO (con copia oculta).

- En el caso de los terceros prestadores de servicios La Administración Pública del Estado de Oaxaca, deben eliminar del correo electrónico de APE cualquier nombramiento o cargo alusivo a para las Dependencias y Entidades del Estado.

- La Dirección General de Tecnologías e Innovación Digital, deberá mantener almacenados los mensajes de correo electrónico por un periodo de cinco años.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

3.4 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por la Dirección General de Tecnologías e Innovación Digital.

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Definición de Términos

Término	*Definición*
Intercambio	Canjear, cambiar algo recíprocamente y que puede darse entre varias personas, organismos, instituciones o naciones. Comunicación que se establece entre dos o más partes para conseguir de parte de la otra algo que se valora.

7.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

SERVICIOS DE COMERCIO ELECTRÓNICO

Referencia ISO 27001:2005. A.10 Gestión de Comunicaciones y Operaciones. A.10.9 Servicios de comercio electrónico.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.10.9 A.10.9.3	*Servicios de comercio electrónico.* Información puesta a disposición pública	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Información puesta a disposición pública.

Objetivo

Establecer las condiciones de uso y controles para poner información a disposición pública

1.0 Propósito

Establecer las condiciones de uso, aprovechamiento, alcances y controles para reducir los riesgos de incidentes de seguridad en disposición pública de la información propiedad y patrimonio del Estado que en medios electrónicos de encuentre.

2.0 Ámbito de Aplicación

Esta política aplica para todas las computadoras y servidores, tanto los arrendados o propiedad de la DGTID, instalados y en operación tanto en las instalaciones de la APE como de otras instalaciones externas a las que se tenga acceso, utilizados por empleados del Estado

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

de Oaxaca, proveedores, usuarios o externos que deban tener acceso a los sistemas de información o servicios de información de la DGTID

3.0 Política

3.1 Descripción de la Política

INFORMACIÓN PUESTA A DISPOSICIÓN PÚBLICA

- La información deberá obtenerse, procesarse y proporcionarse de acuerdo a la normativa vigente, la *Ley de Protección de Datos Personales*.
- La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, deberá ser procesada en forma completa, exacta y oportuna.
- La información sensible deberá ser protegida durante su proceso de recolección y almacenamiento.
- Deberá garantizarse la validez y vigencia de la información publicada.
- La información crítica como parámetros de configuración, arquitectura de software, arquitectura de redes, descripción de componentes, descripción de servicios – equipos, y cualquier información respecto al diseño, código y funcionalidad de los sistemas del Estado, no es sujeta de disposición pública.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

3.4 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por La Dirección General de Tecnologías e Innovación Digital.

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Intercambio	Canjear, cambiar algo recíprocamente y que puede darse entre varias personas, organismos, instituciones o naciones. Comunicación que se establece entre dos o más partes para conseguir de parte de la otra algo que se valora.
Disposición Pública	Que se encuentre disponible para consulta de cualquier persona.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

CONTROL DE ACCESO

GESTIÓN DE ACCESO A USUARIO

Referencia ISO 27001:2005. A.11 Control de Acceso, 11.2 Gestión de acceso de usuario

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión concluido***
A.11.2 A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.4	Gestión de acceso de usuario Registro de usuario Gestión de Privilegios Gestión de contraseñas de usuario Revisión de los derechos de acceso de usuario	2	2.0	En Revisión
Vigencia a partir de:		**Marzo 2019**		

Título de la política

Política de administración de claves y contraseñas para el acceso a los sistemas de bases de datos, sistemas de información y servicios de información.

Objetivo

Establecer los criterios de administración de claves y contraseñas para su protección física y lógica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

1.0 Propósito

Esta política se refiere a los requisitos para el almacenamiento, recuperación y administración segura de las claves de acceso y contraseñas de los usuarios para el uso de bases de datos, sistemas de información y/o servicios de información, así como uso o ejecución de cualquier programa o sistema que deba tener acceso dentro de la red del uso y aprovechamiento de Tecnologías de la Información o de su ámbito de responsabilidad.

Los programas de computadora en ejecución dentro de la red del uso y aprovechamiento de Tecnologías de la Información frecuentemente requieren del uso de los servidores de bases de datos, de sistemas de información o servicios de información. El acceso a estas bases de datos debe efectuarse mediante autenticación a los sistemas o programas a través de la validación de credenciales aceptables. Los privilegios que el o los sistemas asignan a las credenciales pueden comprometerse, así como las restricciones asociadas, cuando las credenciales son almacenadas y/o administradas de forma inapropiada.

2.0 Ámbito de Aplicación

Esta política aplica para todos y cada uno de los sistemas de bases de datos, sistemas de información y servicios de información, así como a paquetes, programas o software en general instalado y en operación dentro o administrado y/o utilizado por o para el uso y aprovechamiento de Tecnologías de la Información al que tendrá acceso el personal de la DGTID.

3.0 Política

Con el objeto de mantener la seguridad para el acceso a los sistemas de bases de datos, sistemas de información y/o servicios de información de la DGTID, el acceso a los programas debe ser otorgado únicamente mediante el procedimiento de autenticación de credenciales.

La credencial empleada para esta autenticación no debe residir en o los programas compilados, en el código fuente o código objeto en texto claro. Las credenciales de los usuarios no deben almacenarse en cualquier equipo o dispositivo al cual se pueda tener acceso a través de web o Internet.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.1 Descripción de la Política

REGISTRO DE USUARIO

- Para llevar a cabo el registro, el usuario deberá generar una solicitud formal a la DIRECCIÓN DE SERVICIOS TECNOLÓGICOS.
  Los responsables del registro de usuarios (administradores de servicios de plataforma o dueño del activo), deberán efectuar el procedimiento de alta o baja, para otorgar y/o revocar el acceso a todos los sistemas, bases de datos y servicios información multiusuario.

- La solicitud y activación de la clave de acceso a los sistemas aplicativos de la Dirección General de Tecnologías e Innovación Digital, es *responsabilidad del dueño del activo* (sistema), por lo que deberá efectuarse dicha solicitud al área responsable del sistema al que se requiera tener acceso.

- El acceso físico a la terminal estará restringido a aquellos empleados que necesitan conocer la información, cuando se utilice la identificación de la terminal para autentificar la conexión.
- No se efectuará el registro de usuario, hasta que se garantice que se han completado los procedimientos de autorización

GESTIÓN DE PRIVILEGIOS

- Para generar el registro de usuario, los dueños del activo entregarán a los usuarios un detalle escrito de sus privilegios y obligaciones en cuanto al acceso.

- Los privilegios de todos los usuarios de la infraestructura tecnológica de todos los usuarios de sistemas, programas y telecomunicaciones deberán ser restringidos.

- Se deberá limitar y controlar la asignación y uso de privilegios, evitando así el uso inadecuado de los mismos y previendo accesos ilegales.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

GESTIÓN DE CONTRASEÑAS DE USUARIO

Almacenamiento de las claves de acceso y contraseñas a las bases de datos

- El Administrador debe efectuar el alta o registro de una nueva(s) cuenta(s) de usuario a los sistemas de información, servicios de información o acceso a la infraestructura tecnológica de la DGTID, previa solicitud formal a las áreas de negocio de la APE dueñas de los sistemas o bien del área de adscripción del solicitante.

- El administrador deberá efectuar la inhabilitación de una cuenta para acceso al o los sistemas de información previa notificación del área de Recursos Humanos, del Jefe Inmediato Superior y/o el dueño del activo.

- El administrador estará obligado a supervisar el contenido de la cuenta de un usuario para verificar que la inhabilitación no afectará información confidencial o de utilidad para las áreas de negocio involucradas.

- Las claves de acceso y contraseñas deben almacenarse en un archivo separado del o los programas compilados, código objeto o código fuente de la aplicación. Este archivo no debe ser legible y debe estar encriptado.

- Las credenciales de acceso a los sistemas y/o servicios de información deben residir en el servidor de cada sistema de información. En este caso un número hash cifrado de identificación de credenciales debe ser almacenado en el código del programa ejecutable.

- Las credenciales de la base de datos pueden almacenase en un servidor de autenticación, como por ejemplo un servidor LDAP utilizado para la autenticación de usuarios. La autenticación de usuarios de bases de datos puede ocurrir en nombre de un programa como parte del proceso de autenticación en el servidor de autenticación. En este caso, no se deben aplicar soluciones programáticas para el uso de credenciales de acceso a bases de datos o acceso a los sistemas o servicios de información.

- Las credenciales de acceso a los sistemas y/o servicios de información no deben residir en ningún árbol de documentos de un servidor web o con acceso directo desde el exterior vía Internet o con acceso público.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- El acceso mediante los procesos de autenticación no debe permitir el acceso a las bases de datos, sistemas de información y/o servicios de información, únicamente basado en el proceso de autenticación de usuario en el host o cliente remoto

- Las contraseñas o frases de paso empleadas para el acceso a las bases de datos, sistemas de información y/o sistemas de información deben adherirse a la *"Política de administración de claves de acceso y contraseñas".*

- El administrador del sistema deberá llevar a cabo un control por escrito, de las cuentas de usuario existentes y otorgadas para acceso a los sistemas de información y a los servidores.

- El administrador otorgará cuenta de acceso a los usuarios previa autorización y solicitud de su área de adscripción, a la Dirección General de Tecnologías e Innovación Digital. El área solicitante deberá verificar que los permisos solicitados no violen la segregación de funciones, así como que los permisos sean los mínimos necesarios para que el usuario realice sus funciones.

- El administrador otorgará sólo los niveles de permisos mínimos necesarios para que cada usuario pueda realizar sus actividades cotidianas.

- Cada cuenta deberá implementar la política de modificación de claves de acceso (password) de forma periódica y obligada.

- La clave de acceso asignada a cada usuario deberá estar formada por letras, números y símbolos con una longitud mínima de 8 caracteres.

Recuperación de Claves y Contraseñas de Acceso a Bases de Datos

- Si no se almacenan en un archivo del código fuente, entonces las claves y contraseñas de usuarios deben leerse desde un archivo inmediatamente antes de su uso. Una vez que haya ocurrido la autenticación por parte de la base de datos, a los sistemas o servicios de información, la memoria que contiene las claves y contraseñas debe borrarse o limpiarse.

- El ámbito o espacio lógico en que las claves y contraseñas de acceso a los sistemas y/o servicios de información, debe estar físicamente separado de otras áreas del código.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Por ejemplo, las credenciales deben estar en un archivo fuente distinta. El archivo que contienen las claves y contraseñas no debe contener nada más que el código de las credenciales y cualquier función, rutina o método que será empleado exclusivamente para el acceso de las credenciales.

- Para lenguajes que se ejecuten desde el código fuente, el archivo de credenciales no debe residir en el mismo árbol de directorio del archivo ejecutable y el cuerpo del código ejecutable.

Claves y Contraseñas de Acceso a los Sistemas de Bases de Datos

- Cada programa o colección de programas que efectúen una sola función de negocios deben tener una única y exclusiva base de datos de credenciales. No se debe permitir el uso compartido de credenciales entre programas o sistemas. Es decir, cada sistema debe contar con su propia base de datos de credenciales de usuarios.

- Las claves de acceso y contraseñas empleados por los programas o sistemas deben ser a nivel de sistema tal y como se definen en *"Política de administración de claves de acceso y contraseñas".*

- Los programadores y desarrolladores deben implementar un proceso para asegurar que las claves de acceso y contraseñas se asignen y modifiquen de acuerdo con la *"Política de administración de claves de acceso y contraseñas".* Este proceso debe incluir un método de restricciones para el acceso y distribución de claves y contraseñas.

Vigencia de Claves y Contraseñas de Acceso a los Sistemas de Bases de Datos

- El usuario deberá cambiar la contraseña genérica entregada en el primer inicio de sesión.
- La contraseña deberá bloquearse al quinto intento fallido.
- La contraseña deberá cambiarse cada 180 días excepto las cuentas de la administración y servicios de Tecnologías de la Información que será cada 30 días.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Técnicas de Codificación para la Implementación de esta Política

- Se deberán incorporar las referencias específicas de las guías de seguridad para cada uno de los diferentes lenguajes de programación tales como Perl, Java, C, C++, Visual Basic, o cualquier lenguaje empleado con el objeto de crear, mantener y administrar las claves de usuario y contraseñas de forma segura, tanto para la aplicación como para el proceso de administración.

REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIO

- Los administradores de la plataforma de tecnología de la información revisarán los derechos de acceso de los usuarios periódicamente, no excediendo de seis meses cada revisión.

- Los privilegios en el acceso a los datos, servicios de información y de comunicaciones de todos los usuarios, deberán revisarse, con la finalidad de detectar comportamientos anormales o inactividad, a fin de garantizar que no se obtengan privilegios no autorizados

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TICs, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

3.4 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por la Dirección General de Tecnologías e Innovación Digital.

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Nivel de violación y sanción por incumplimiento a los criterios de esta política: 6

5.0 Definición de Términos

Término	***Definición***
Lenguaje de programación	Lenguaje intérprete o compilado para la generación de programas y/o sistemas.
Credenciales	Algo que el usuario conoce (clave de acceso y contraseña), algo que identifica al usuario (nombre de usuario, huella dactilar, huella de voz o huella de retina) o algo que identifica al usuario y que es presentado para una autenticación.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Término	*Definición*
Derecho	El nivel de privilegio que se deriva del proceso de autenticación y autorización. Nivel de privilegio para el acceso a los recursos.
Programa ejecutable	Código, rutinas o instrucciones de máquina que la computadora ejecuta para correr un programa.
Hash	Número generado por un algoritmo que identifica un dato o su localización.

Término	**Definición**
LDAP	Protocolo de Acceso a Directorio Ligero – Lightweight Directory Access Protocolo -, conjunto de protocolos de acceso a información de directorios.
Módulo	Colección o conjunto de instrucciones de computadora agrupados de forma conjunta tanto lógica como físicamente. Un módulo puede también referirse a un paquete o clase, dependiendo del lenguaje de desarrollo empleado.
Espacio de nombres	Área lógica de código en el cual los nombres simbólicos declarados son conocidos y fuera de esa área, esos nombres no son visibles para el resto del código.
Producción	Software que está siendo utilizado para propósitos diferentes a la implementación o pruebas.
Vigencia	Lapso en que puede ser utilizada y tiene validez.
Usuario	Persona que utiliza los sistemas informáticos de la DGTID al que se le ha proporcionado una “Cuenta de usuario asociada a una contraseña”, siendo estos administrados por el Directorio Activo de la DGTID. Por lo que en el APE no existe la figura de “Usuario” que no tenga acceso al uso de internet o correo electrónico.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

RESPONSABILIDADES DEL USUARIO

Referencia ISO 27001:2005. A.11 Control de Acceso A.11.3 Responsabilidades de usuario.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.11.3 A.11.3.1 A.11.3.2 A.11.3.3	Responsabilidades de usuario Uso de contraseña Equipo se usuario desatendido Política de puesto de trabajo despejado y pantalla limpia	2	2.0	Concluida
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Responsabilidades de los usuarios en uso y aprovechamiento de las Tecnologías de la Información y Comunicaciones.

Objetivo

Establecer las responsabilidades que los usuarios deben cumplir en cuanto al uso de contraseña, la seguridad del equipo y del lugar de trabajo.

1.0 Propósito

Esta política se refiere a los requisitos mínimos indispensables que deben cubrir los usuarios en cuanto al uso y aprovechamiento de Tecnologías de la Información, respecto a las contraseñas, la atención del equipo con el que trabaja, a mantener su puesto de trabajo despejado y su pantalla limpia. Estas responsabilidades tienen por objeto reducir el riesgo de acceso no autorizado o daño a los papeles de trabajo y medios de procesamiento de la información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica para todos y cada uno de los usuarios de tecnologías de la Información de cada una de las áreas que conforman el APE.

3.0 Política

3.1 Descripción de la Política

USO DE CONTRASEÑA

- Los usuarios deberán seguir buenas prácticas de seguridad en la selección y uso de **contraseñas** con las que operen en su ámbito de trabajo, debido a que constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

- Los usuarios no deberán crear una contraseña que sea obvia, predecible o deducible, como detalles personales, fechas de nacimiento, secuencias de números o caracteres comunes, etc., además deberá utilizar distintas contraseñas en cada uno de los sistemas para los que se les ha otorgado el acceso. Deberá evitar reutilizar o reciclar viejas contraseñas.

- Los usuarios deben mantener las contraseñas en secreto, entendiendo que su uso es personal e intransferible y por ende en su responsabilidad el uso que se dé de ella.

- Los usuarios son responsables de su contraseña y se comprometen a no compartirla, prestarla o intercambiarla

- Los usuarios deberán solicitar o efectuar cambio de la contraseña, cuando considere que ha sido divulgada o existe un riesgo en los sistemas donde la utiliza.

- Los usuarios deberán cambiar las contraseñas provisorias en el primer inicio de sesión ("log on") y evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

EQUIPO DE USUARIO DESATENDIDO

- Los usuarios deberán garantizar mediante la salida del sistema o invocar un protector de pantalla, que sus computadores personales, estaciones de trabajo o terminales no queden desatendidos.

- Los equipos que permanezcan desatendidos por un periodo mayor a 10 minutos serán bloqueados automáticamente mediante el protector de pantalla protegido con contraseña.

- Los usuarios no deberán abandonar su estación de trabajo con el inicio de sesión activo, deberán bloquear su equipo siempre que se retiren de su lugar de trabajo.

- En caso de que los computadores personales se encuentren conectados a una red, siempre deben estar fuera de sistema si se van a encontrar desatendidos por el usuario.

- Los usuarios deberán concluir las sesiones activas al finalizar sus tareas, o bien utilizar un mecanismo de bloqueo adecuado como un protector de pantalla protegido por contraseña, cuando suspenda sus actividades por un lapso corto de tiempo.

- Los usuarios deberán proteger sus equipos o terminales mediante contraseña de acceso, de esta forma se protegen los equipos contra usos no autorizados.

- La Dirección de Servicios Tecnológicos, debe coordinar con la Jefatura de Servicios de Recursos Humanos, una campaña de las tareas de concientización a todos los usuarios y terceros, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación con la implementación de dicha protección.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

- Es responsabilidad del personal de la DGTID, el uso indebido que se dé a la información con que trabaja, ya sea en medios electrónicos o impresos, por ende, debe mantener su lugar de trabajo despejado, en caso de que no se encuentre trabajando en dicho sitio.

- Las políticas señaladas en el apartado de *Equipo de usuario desatendido*, deberán aplicarse para lo relativo a pantalla limpia.

- En este apartado aplican las políticas de *Clasificación de Información* que está dentro del rubro de *Gestión de Activos*.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.3 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

3.4 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por la Dirección General de Tecnologías e Innovación Digital.

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Contraseña	Palabra clave que se utiliza para tener acceso a un equipo o sistema.
Sesiones Activas	Sesión de trabajo en la que se encuentra el usuario operando.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones históricas de la política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

USO ACEPTABLE DE LOS RECURSOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES REMOTAS

Referencia ISO 27001:2005. A.11 Control de Acceso A.11.4 Control de Acceso a la Red

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.11.4 A.11.4.1 A.11.4.2	Control de acceso a la red Políticas de uso de los servicios en red Autenticación de usuario para conexiones externas	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Política de uso de los recursos de tecnologías de la información y comunicaciones remotas.

Objetivo

Definir las restricciones en el uso de la infraestructura tecnológica del uso y aprovechamiento de Tecnologías de la Información, así como al medio de conexión remota con los recursos de la información del Estado de Oaxaca.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

1.0 Propósito

El propósito de esta política es controlar las acciones para conectarse con la red y/o recursos de infraestructura tecnológica, a través de cualquier equipo de cómputo o dispositivo. Estas restricciones se diseñan para reducir al mínimo la exposición potencial del uso y aprovechamiento de Tecnologías de la Información, por los daños que pueden resultar del uso no autorizado de los recursos de la DGTID Los daños incluyen la pérdida de datos confidenciales sensibles de para las Dependencias y Entidades del Estado, de propiedad intelectual, daño a la imagen pública, los sistemas internos críticos, los sistemas de información, servicios de información o a cualquier otro tipo de dato, información o dispositivo propiedad de la DGTID

2.0 Ámbito de Aplicación

Esta política se aplica a todos los empleados del uso y aprovechamiento de Tecnologías de la Información, contratistas, vendedores, proveedores, usuarios y/o externos que poseen una computadora personal o de escritorio y/o dispositivo y que son usadas para conectarse con la red del Estado. Esta política aplica al acceso local y/o remoto a las conexiones usadas para hacer el trabajo a nombre del uso y aprovechamiento de Tecnologías de la Información, incluyendo la lectura o el enviar correo electrónico y uso de recursos de Intranet o Internet.

3.0 Política

3.1 Descripción de Política

- El personal de la Dirección General de Tecnologías e Innovación Digital, debe establecer por todos los medios, métodos, procesos, procedimientos y tecnologías disponibles y a su alcance, de las restricciones necesarias a los equipos y/o dispositivos que sean instalados y/o conectados a los recursos de la Red de Servicios del Estado, así como la definición de roles, perfiles y permisos que sea estrictamente indispensables y mínimos para el cumplimiento de las labores encomendadas al personal que labore tanto para La Administración Pública del Estado de Oaxaca como para usuarios, proveedores y terceros que tengan relación laboral, contractual, comercial o institucional con la APE.

- Es responsabilidad de los empleados del uso y aprovechamiento de Tecnologías de la Información, de contratistas, proveedores, usuarios y de agentes externos con privilegios de acceso local y/o remoto a la red corporativa de asegurarse de que su conexión del acceso está sujeta a las restricciones definidas por la DGTID para ese perfil específico.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- El acceso general a internet para el uso recreacional, en los computadores personales está prohibido. El empleado es responsable de garantizar el no violar ninguna de las políticas, que no realiza actividades ilegales, y no utiliza el acceso para otros fines que no sean institucionales.

- Se debe verificar las políticas relacionadas a los detalles sobre protección de la información al tener acceso a la red institucional mediante métodos de acceso remoto, así como a la política de uso aceptable de la red de la DGTID

- Para solicitar algún servicio relacionado con los recursos de tecnologías de la información y/o comunicaciones remotas, se deberá enviar un oficio y/o correo electrónico a la Dirección General de Tecnologías e Innovación Digital, quien a su vez y de proceder será canalizada a la mesa de servicios para su atención.

3.2 Requisitos

- Los accesos remotos deben ser controlados estrictamente. El control se debe cumplir mediante la autentificación de una sola vez de la contraseña o a través de algún método de llaves públicas y privadas. Para la información sobre crear una contraseña fuerte vea la *política de la contraseña.*

- En ninguna hora ni un empleado proporcionará su conexión o contraseña a través del correo electrónico o cualquier medio físico o lógico a cualquier persona.

- Los empleados y los contratistas con privilegios del acceso remoto deben asegurarse de que su laptop o computadora de escritorio al momento en que están conectados remotamente con la red corporativa del uso y aprovechamiento de Tecnologías de la Información, no se encuentren conectados con ninguna otra red exactamente al mismo tiempo o de forma simultánea, a excepción de las redes personales que están bajo control completo del usuario.

- Los empleados y proveedores o terceros, con privilegios del acceso remoto hacia a la red de servicios del Estado, no deben utilizar las cuentas del correo electrónico de terceros (ejemplo, Hotmail, Yahoo, Gmail, AOL), u otros recursos externos para comunicaciones del Estado y sus Dependencias, con el objeto de asegurar que el negocio e interés oficial nunca debe confundirse con los intereses personales.
- Los ruteadores para las líneas dedicadas de comunicaciones de voz y/o datos configuradas para el acceso a la red deben incorporar los requisitos mínimos de la autentificación.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Se prohíbe totalmente y sin excepción, la configuración de equipos comerciales con el fin de tener acceso privilegiado a los recursos de información o de la red de servicios del Estado, para cualquier persona perteneciente o ajena a la Administración Pública del Estado o de la DGTID.

- Las configuraciones de hardware no estándar. se deben aprobar para el servicio de acceso remoto a la red o redes del Estado; por lo tanto, la Dirección de Servicios Tecnológicos debe aprobar las configuraciones de seguridad para el acceso al hardware.

- Todos los equipos que están conectados con las redes internas vía tecnologías del acceso remoto deben utilizar el software más actualizado de antivirus, esto incluye a los equipos personales.

- El equipo personal que se va a emplear para conectarse de forma remota con la red o redes del uso y aprovechamiento de Tecnologías de la Información, debe cubrir los requisitos de seguridad establecidos para tal efecto.

- Las organizaciones o individuos que deseen incorporar soluciones no estándares para el acceso remoto a la red de producción del Estado, deben obtener la aprobación correspondiente por parte de la Dirección de Servicios Tecnológicos.

3.3 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.4 Monitoreo

La Jefatura de la Unidad de Planeación y Control de TIC´s, deberá realizar una revisión y seguimiento permanente al cumplimiento de esta política en la elaboración, modificaciones y actualizaciones a las políticas de seguridad de la información.

3.5 Revisiones y Auditorías

Las revisiones y/o auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto por la DGTID.

Las auditorías serán administradas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	*Definición*
Comunicación remota	Cualquier medio o dispositivo para realizar una comunicación y/o transmisión de datos con la red o redes de la APE desde una localidad externa a las instalaciones del Estado de Oaxaca.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

INSTALACIÓN Y ADMINISTRACIÓN DE SERVIDORES

Referencia ISO 27001:2005. A.11 Control de Acceso. A.11.4 Control de Acceso a la Red.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, en revisión y concluido***
A.11.4 A.11.4.6	Control de acceso a la red Control de la conexión a la red	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Política de instalación y administración de servidores.

Objetivo

Establecer los criterios y controles para la instalación y administración de servidores en operación dentro de la red o redes que administra y custodia la DGTID

1.0 Propósito

El propósito de esta política es establecer los estándares para la configuración básica de instalación y administración de servidores internos que son propiedad y/o que se encuentran instalados y operados por la DGTID. La implementación efectiva de esta política debe disminuir los riesgos por accesos no autorizados a los medios de información y/o a la tecnología propiedad del Estado.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica a los servidores registrados bajo el dominio de red interno en custodia de la DGTID. Esta política es específica para los equipos ubicados en la red interna en administración de la DGTID.

3.0 Política

3.1 Descripción de Política

- Todos los servidores internos y en operación dentro de la administración de la DGTID, deben ser administrados exclusivamente por los administradores designados por la Dirección de Servicios Tecnológicos. La guía de configuración de servidores aprobada, debe ser establecida y mantenidas por el personal responsable de la administración de los servidores. Esta guía de configuración debe estar basada en las necesidades de negocio de la DGTID. El o los administradores deben efectuar el monitoreo y cumplimiento de cada configuración e implementar las políticas de excepción apropiadas para cada ambiente. Se debe establecer un proceso para el cambio en la guía de configuración, la cual debe ser revisada y aprobada por la dirección de sistemas de la DGTID
- Cada uno de los servidores debe ser registrado dentro del sistema de administración de la DGTID. Así mismo, debe registrarse un mínimo de información para la total identificación de un punto de contacto tales como:

    - Marca, modelo y características generales de cada servidor (memoria RAM, procesador (interfaz, modelo, velocidad, unidades de disco, espacio en disco de cada unidad, sistema operativo, versión y versión de la última actualización).
    - Dirección(es) IP, tipo de interface de red, diagrama de topología dentro de la red(es) de para las Dependencias y Entidades del Estado.
    - Funcionalidad principal y servicios de información configurados y en operación en cada servidor.
    - Programas, sistemas, aplicaciones y cualquier software instalado en el servidor con funcionalidad independiente al sistema operativo y que otorgue servicios a los usuarios (ejemplo, dns, correo, dhcp, https, etc.).
    - Programas, procesos, procedimientos, características, ubicación e información de las unidades, cartuchos y/o cintas de respaldos por cada servidor.
    - Los cambios que se realicen en los servidores de producción deben efectuarse a través de los procedimientos apropiados de administración de cambios y con el formato correspondiente.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Guía general de Configuración de Servidores

- La instalación del sistema operativo de cada servidor deberá realizarse con los criterios de eficiencia y seguridad, así como la instalación de aplicaciones y servicios de acuerdo a su función o funciones específicas (impresión, controlador de dominio, bases de datos, servicios web, etc.).
- La configuración del sistema operativo debe ser en total concordancia con las guías de configuración aprobadas por la Dirección General de Tecnologías e Innovación Digital.
- Todos los servicios y aplicaciones que no son indispensables para la operación y administración de los servidores, así como para su funcionalidad principal deben ser inhabilitadas o desinstaladas.
- El administrador deberá inhabilitar o desinstalar cualquier protocolo que no sea indispensable para la operación adecuada del servidor y del acceso de los usuarios al mismo.
- El acceso a los servicios debe ser a través de un nombre de usuario y clave de acceso, protegidos por métodos de control de acceso tales como TCP Wrappers, Kerberos o técnicas similares si es posible.
- Deben de instalarse y configurarse los parches de seguridad o actualizaciones a la última versión posible y disponible tan pronto como sea práctico y recomendable, y la única excepción será cuando su aplicación inmediata pudiera representar una seria interferencia con los requerimientos del negocio o con la operación de los servicios ya en producción.
- Las relaciones de confianza entre sistemas representan un riesgo de seguridad y su empleo debe ser restringido. No se debe emplear una relación de confianza entre servidores cuando exista otro método para ello que implique mayor seguridad.
- Siempre se debe emplear el principio de los mínimos privilegios necesarios requeridos para el acceso a los servidores con el objeto de desempeñar cualquier función operativa y/o administrativa.
- Nunca se debe usar la cuenta de administrador para realizar tareas de mantenimiento, cuando una cuenta con menos privilegios lo debe hacer.
- Si existiera cualquier método disponible para una conexión en un canal seguro (si fuera técnicamente posible) el acceso privilegiado debe realizarse siempre por medios de canales seguros cifrados (por ejemplo, el empleo de conexiones de red cifradas usando SSH o IPSec).
- Todos y cada uno de los servidores deben estar instalados en un ambiente de acceso controlado.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- La administración de los servidores debe estar específicamente prohibido desde áreas no controladas por el personal de la Dirección General de Tecnologías e Innovación Digital de la DGTID
- El administrador de sistemas deberá establecer las funciones básicas, principales e indispensables de cada servidor e instalar exclusivamente las aplicaciones y servicios que estén acordes con las funciones básicas de cada servidor.
- El administrador deberá probar e instalar los paquetes de servicio correspondiente a cada servidor, así como las últimas actualizaciones y revisiones provistas por el fabricante de cada sistema operativo.
- El administrador deberá supervisar constantemente y de forma permanente, las liberaciones de las últimas versiones de paquetes de servicio y parches a los sistemas operativos instalados y en operación.
- El administrador deberá estudiar y analizar la información proporcionada por el fabricante de los sistemas operativos, sobre los paquetes de servicio y parches con el objeto de disminuir riesgos por la implementación inadecuada de los mismos.
- El administrador podrá omitir la instalación de cualquier parche o paquete de servicio que pueda ocasionar problemas o inestabilidad en los sistemas de información y deberá reportarlo en la bitácora correspondiente.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.3 Monitoreo

Todos los eventos de seguridad relacionados a sistemas críticos o sensibles en la operación, deben ser registrados en las bitácoras (logs) y auditados de la siguiente manera:

- Todas las bitácoras de seguridad deben mantenerse en línea por lo menos una semana.
- Las cintas de respaldos incrementales deben ser mantenidas sin cambios o reescrituras por lo menos un mes.
- Los respaldos totales semanales de las bitácoras deben ser resguardadas por lo menos un año.

Los eventos e incidentes de seguridad deben reportarse a la Dirección de Servicios Tecnológicos y gestionarse mediante el proceso de gestión de incidentes. Las medidas correctivas serán determinadas de acuerdo con el riesgo y severidad de estas. Los incidentes de seguridad incluyen, pero no están limitados por:

- Ataques de rastreo de puertos.
- Evidencia de acceso no autorizado mediante cuentas privilegiadas.
- Ocurrencias anómalas que no están relacionadas con la operación normal de ninguna aplicación específica.
- Transmisiones de paquetes que tengan como origen al servidor y que no formen parte de la operación y/o administración normal y justificada.
- Alteración o modificación de la información contenida en el servidor sin razón justificada al sistema operativo, programas, paquetes, software, bases de datos, información o datos que formen parte de los elementos de administración, operación o mantenimiento del mismo.

3.4 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto.

Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Nivel de violación y sanción por incumplimiento a los criterios de esta política: 6

5.0 Definición de términos

Término	***Definición***
DMZ	En seguridad de la información, una zona desmilitarizada (DMZ, De Militarized Zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.
Servidor	Para los propósitos de esta política específica, un servidor se define como un equipo servidor instalado y en operación en el uso y aprovechamiento de Tecnologías de la Información que proporciona el proceso de medios o servicios de información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López Director *General* *Dirección General de Tecnologías e Innovación Digital*	Ing. Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

CONTROL DE ACCESO AL SISTEMA OPERATIVO

Referencia ISO 27001:2005. A.11 Control de Acceso. A.11.5 Control de Acceso al sistema operativo.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.11.5	Control de Acceso al sistema operativo	2	2.0	En proceso
A.11.5.1	Procedimientos seguros de inicio de sesión			
A.11.5.2	Identificación y autenticación de usuario			
A.11.5.3	Sistema de Gestión de contraseñas			
A.11.5.5	Desconexión automática de sesión			
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Sistema de Gestión de contraseñas.

Objetivo

Establecer los criterios necesarios para que los Administradores de los Sistemas y/o Servicios de la Dirección de Servicios Tecnológicos de la DGTID, lleven a cabo con la finalidad de administrar y mantener la seguridad de la información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

1.0 Propósito

El propósito de esta política es establecer los criterios necesarios para que los Administradores de los Sistemas y/o Servicios de la Dirección de Servicios Tecnológicos de la DGTID, lleven a cabo dentro de sus actividades cotidianas, a fin de disminuir los riesgos de accesos no autorizados a los medios de información y/o a la tecnología propiedad de la DGTID

2.0 Ámbito de Aplicación

Esta política aplica para que los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, equipos servidores bajo el dominio de red interno propiedad de la DGTID.

Esta política es específica para los equipos ubicados en la red interna de la DGTID

3.0 Política

3.1 Descripción de Política

PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN

- Respecto a los Intentos de introducir contraseña, una vez que los usuarios cubren cinco intentos infructuosos por introducir su contraseña, esta quedará bloqueada o desactivada durante quince minutos como parte de los procedimientos seguros de inicio de sesión.
- Mediante procedimientos de seguridad y/o protocolos, se efectúa un control de acceso a la información seguro de inicio de sesión, estableciendo una relación de confianza entre el equipo cliente y el servidor.

IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIO

- Todos los usuarios (incluido el personal de TI), tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que sus actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no deberán dar ningún indicio del nivel de privilegios otorgados.

SISTEMA DE GESTIÓN DE CONTRASEÑAS

- La clave de acceso de los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, deberá estar constituida por ocho dígitos como mínimo, incluyendo mayúsculas, minúsculas y números.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, deberán cambiar sus claves de acceso cada treinta días (30).

- Las claves de acceso de los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, deberán ser generadas en un archivo protegido y enviado vía correo electrónico a la Jefatura de Informática, Base de Datos y Seguridad dependiente de la Dirección de Servicios Tecnológicos, los primeros días del mes, a más tardar el quinto día hábil de cada mes

- La Jefatura de infraestructura, Base de Datos y Seguridad dependiente de la Dirección de Servicios Tecnológicos de la DGTID, deberá mantener resguardados los archivos de cada administración de servicios, conteniendo las claves de acceso.

- En caso de presentarse una contingencia, los archivos que contienen las claves de acceso de los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, serán accesados en presencia del Jefe de Unidad o Departamento de TI o de algún jefe de departamento de dicha área.

- Se registrará en una bitácora, una vez que se llegue a accesar dichos archivos, especificando la razón y firmando de conformidad el Jefe de Unidad o Departamento de TI o de algún jefe de departamento de dicha Jefatura de Servicios y el administrador de sistemas o servicios al que pertenezca dicha clave de acceso.

DESCONEXIÓN AUTOMÁTICA DE SESIÓN

- Las Pc´s se bloquearán después de un periodo definido de inactividad o tiempo muerto, para evitar el acceso de personas no autorizadas. Este bloqueo por tiempo muerto deberá limpiar la pantalla.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Monitoreo

Todos los eventos de seguridad relacionados a sistemas críticos o sensibles en la operación de para las Dependencias y Entidades del Estado, deben ser registrados en las bitácoras (logs) y auditados de la siguiente manera:

- Todas las bitácoras de seguridad deben mantenerse en línea por lo menos una semana.

Los eventos e incidentes de seguridad deben reportarse a la Dirección de Servicios Tecnológicos, quien será el único responsable de revisar las bitácoras y reportar los incidentes correspondientes. Las medidas correctivas serán determinadas de acuerdo con el riesgo y severidad de estas. Los incidentes de seguridad incluyen, pero no están limitados por:

- Ataques de rastreo de puertos.
- Evidencia de acceso no autorizado mediante cuentas privilegiadas.
- Ocurrencias anómalas que no están relacionadas con la operación normal de ninguna aplicación específica.
- Transmisiones de paquetes que tengan como origen al servidor y que no formen parte de la operación y/o administración normal y justificada.
- Alteración o modificación de la información contenida en el servidor sin razón justificada al sistema operativo, programas, paquetes, software, bases de datos, información o datos que formen parte de los elementos de administración, operación o mantenimiento del mismo.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.4 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto.

Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN

Referencia ISO 27001:2005. A.11 Control de Acceso. A.11.6 Control de Acceso a las aplicaciones y a la información.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.11.6 A.11.6.1	Control de Acceso a las aplicaciones y a la información Restricción del acceso a la información	2	2.0	Concluido
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Restricción del acceso a la información.

Objetivo

Establecer los criterios necesarios para que los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, lleven a cabo con la finalidad de administrar y mantener la seguridad de la información.

1.0 Propósito

El propósito de esta política es establecer los criterios necesarios para que los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, lleven a cabo dentro de sus actividades cotidianas, a fin de disminuir los riesgos de accesos no autorizados a los medios de información y/o a la tecnología propiedad del Estado y en custodia de la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica para que los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, equipos, así como los servidores registrados bajo el dominio de red interno propiedad de la DGTID

Esta política es específica para los equipos ubicados en la red interna de la DGTID

3.0 Política

3.1 Descripción de Política

RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

- Los sistemas aplicativos e información generada es propiedad de los dueños del activo, en este caso las áreas usuarias son las responsables directamente del uso que se dé a la información de la que son propietarios. Solo las Áreas Usuarias (propietarias del activo) son las únicas responsables de otorgar los permisos de acceso y restricciones necesarias de estos sistemas mediante la autorización de una cuenta y clave de acceso (lo antes indicado en relación a la restricción específica de acceso a la información y a las aplicaciones de los usuarios y al personal de soporte).

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Monitoreo

Todos los eventos de seguridad relacionados a sistemas críticos o sensibles en la operación de para las Dependencias y Entidades del Estado, deben ser registrados en las bitácoras (logs) y auditados de la siguiente manera:

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Todas las bitácoras de seguridad deben mantenerse en línea por lo menos una semana.

Los eventos e incidentes de seguridad deben reportarse a la Dirección de Servicios Tecnológicos, quien será el único responsable de revisar las bitácoras y reportar los incidentes correspondientes. Las medidas correctivas serán determinadas de acuerdo con el riesgo y severidad de estas. Los incidentes de seguridad incluyen, pero no están limitados por:

- Ataques de rastreo de puertos.
- Evidencia de acceso no autorizado mediante cuentas privilegiadas.
- Ocurrencias anómalas que no están relacionadas con la operación normal de ninguna aplicación específica.
- Transmisiones de paquetes que tengan como origen al servidor y que no formen parte de la operación y/o administración normal y justificada.
- Alteración o modificación de la información contenida en el servidor sin razón justificada al sistema operativo, programas, paquetes, software, bases de datos, información o datos que formen parte de los elementos de administración, operación o mantenimiento del mismo.

3.4 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto. Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

EQUIPOS MÓVILES Y TRABAJO REMOTO.

Referencia ISO 27001:2005. A.7 Ordenadores portátiles y teletrabajo. A.11.7.1 Ordenadores portátiles y comunicaciones móviles.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.11.7 A.11.7.1	Equipos Móviles y trabajo remoto Ordenadores Equipos Móviles	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Seguridad en el uso de equipos móviles y trabajo en remoto.

Objetivo

Establecer los criterios necesarios para que los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, lleven a cabo con la finalidad de administrar y mantener la seguridad de la información, en el uso de equipos móviles y trabajo remoto.

1.0 Propósito

El propósito de esta política es establecer los criterios necesarios para que los Administradores de los Sistemas y/o Servicios de la Dirección de Servicios Tecnológicos de la DGTID, lleven a cabo dentro de sus actividades cotidianas, a fin de disminuir los riesgos de accesos no autorizados a los medios de información y/o a la tecnología propiedad de la DGTID por el uso de equipos móviles y trabajo remoto.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica para que los Administradores de los Sistemas y/o Servicios de la Dirección de Servicios Tecnológicos de la DGTID, equipos servidores propiedad y operados por o para el uso y aprovechamiento de Tecnologías de la Información, así como los servidores registrados bajo el dominio de red interno propiedad de la DGTID

Esta política es específica para los equipos ubicados en la red interna de la DGTID

3.0 Política

3.1 Descripción de Política

COMPUTADORAS PORTÁTILES Y COMUNICACIONES MÓVILES.

- Las computadoras portátiles y comunicaciones móviles deberán tener restricciones de acceso al entorno de la red de cómputo del Estado. El propietario de los mismos deberá solicitar formalmente el acceso a la Dirección de Servicios Tecnológicos, de tal forma que el usuario pueda hacer uso temporal y restringido de los recursos de la red del Estado de Oaxaca en forma remota, controlando así las actividades que llegará a efectuar y evitando a la vez correr algún riesgo potencial (lo antes indicado en relación a la adopción a medidas de seguridad adecuadas de protección contra riesgos de la utilización de computadoras portátiles y comunicaciones móviles).

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.3 Monitoreo

Todos los equipos de cómputo portátiles y comunicaciones móviles deberán monitorearse para que una vez que dejen de prestar sus servicios a APE sean retirados los accesos y permisos concedidos.

3.4 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto. Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

Referencia ISO 27001:2005. A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.12.1 A.12.1.1	Requisitos de seguridad de los sistemas de información Análisis y especificación de los requisitos de seguridad	2	2.0	Concluido
A.12.2 A.12.2.1 A.12.2.2 A.12.2.4	Tratamiento Correcto de las aplicaciones Validación De los datos de entrada Control de procesamiento interno Validación de los datos de salida	2	2.0	Concluido
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Requisitos de seguridad de los sistemas de información.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Objetivo

Establecer, incorporar y mantener la seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de información de la DGTID, así como también, prevenir errores, pérdida, modificación o mal uso de la información, garantizando su seguridad.

1.0 Propósito

El propósito de esta política es establecer, incorporar y mantener la seguridad para la adquisición, desarrollo, procesamiento y mantenimiento de los sistemas de información de la DGTID, mismos que los Diseñadores, Desarrolladores y Administradores de los Sistemas y/o Servicios, de la Dirección General de Tecnologías e Innovación Digital, deberán incorporar y mantener dentro de sus actividades cotidianas, a fin de disminuir los riesgos a que están expuestos los sistemas de información de la APE y garantizar su seguridad.

2.0 Ámbito de Aplicación

Esta política aplica para los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, aun cuando estos sean terceros prestadores al servicio, equipos servidores propiedad y operados por o para La Administración Pública del Estado de Oaxaca, así como los servidores registrados bajo el dominio de red interna propiedad de la DGTID

Esta política aplica para los equipos de hardware y humano ubicados fuera de la red interna del uso y aprovechamiento de Tecnologías de la Información y que se encuentren por cualquier relación contractual bajo la administración de un Tercero.

3.0 Política

3.1 Descripción de Política

REQUISITOS DE SEGURIDAD DE LOS SISTEMA DE INFORMACIÓN

ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD

- Para todos los sistemas de aplicaciones, los arquitectos, analistas, diseñadores y desarrolladores de sistemas deben considerar la seguridad de la información desde el principio del proceso de diseño de los sistemas, cada una de las fases de desarrollo hasta su liberación en producción.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Las áreas usuarias que soliciten el desarrollo de un sistema de información, deberán especificar claramente aquellas medidas de seguridad que requiere contener su sistema, con el fin de que sean considerados desde el análisis y diseño del mismo.
- Durante la fase de análisis de requerimientos se deben identificar los requerimientos de validación de datos como: caracteres inválidos, información incompleta y datos fuera de rango.
- El dueño del activo debe validar con el Arquitecto de Software y el Oficial de Seguridad de la Información los requerimientos y controles de seguridad a implementar.
- Se deberán analizar los requerimientos de capacidad y recursos de los nuevos desarrollos, con el fin de garantizar que no existan fallas una vez implementados en producción.
- Antes de poner en producción algún sistema de información, deberán verificarse los requisitos de seguridad.
- Los productos de seguridad que pretendan utilizarse en los sistemas de información, deben evaluarse previamente a la adquisición de los mismos, de tal forma que sea posible reconsiderarlos en caso de que no cubran las expectativas y/o necesidades preestablecidas.

METODOLOGÍA

Se debe contar con una metodología de desarrollo estándar y documentada. Esta metodología debe incluir de manera enunciativa más no limitativa:

- Reglas para las fases de estudio de factibilidad, diseño, construcción, pruebas, implementación y revisiones post-implementación de la satisfacción del usurario final.
- Análisis de Riesgos.
- Participación de los usuarios en la etapa de diseño y pruebas.
- Entrenamiento y documentación de usuario y operación.
- Control de calidad.

TRATAMIENTO CORRECTO DE LAS APLICACIONES

VALIDACIÓN DE LOS DATOS DE ENTRADA

- Los usuarios de los sistemas de información no deberán tener privilegios para modificar los datos de producción.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Los sistemas de información de la DGTID, deben ser construidos de manera que ninguna persona esté en posibilidades de manipular los registros sin que dichos eventos sean detectados y queden registrados.
- Deben establecerse mecanismos, controles y/o procedimientos que aseguren que todas las entradas a los sistemas de producción que han sido enviadas para su procesamiento hayan sido autorizadas adecuadamente, así como, validar toda la información sensible o crítica procesada y de salida.
- Se definirá un procedimiento que, durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados.

CONTROL DE PROCESAMIENTO INTERNO

- Una vez terminada la etapa de desarrollo se deben realizar revisiones del código para verificar que no existan puertas traseras o rutinas que comprometan la integridad y confidencialidad de la información o la disponibilidad de la aplicación.
- Una vez validado y entregado el sistema o aplicación, se hará la entrega del código fuente al Oficial de Seguridad de la Información, debiendo observar la integración de toda la información documental a la que haya a lugar en relación con el sistema o aplicación.
- Todo desarrollo desde su diseño hasta su liberación y puesta en producción es total e íntegramente propiedad de la Dirección General de Tecnologías e Innovación Digital.

VALIDACIÓN DE LOS DATOS DE SALIDA

- Toda información y/o datos de salida para el tratamiento correcto de las aplicaciones, deben pasar por una validación y control con la finalidad de cuidar la integridad y confiabilidad de los mismos, evitando con ello errores, perdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones (lo antes indicado en relación a la validación para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias).

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Monitoreo

Todos los eventos de seguridad relacionados a sistemas críticos o sensibles en la operación de para las Dependencias y Entidades del Estado, deben ser registrados en las bitácoras (logs) y auditados de la siguiente manera:

- Todas las bitácoras de seguridad deben mantenerse en línea por lo menos una semana.

Los eventos e incidentes de seguridad deben reportarse a la Dirección de Servicios Tecnológicos, quien será el único responsable de revisar las bitácoras y reportar los incidentes correspondientes. Las medidas correctivas serán determinadas de acuerdo con el riesgo y severidad de las mismas. Los incidentes de seguridad incluyen, pero no están limitados por:

- Ataques de rastreo de puertos.
- Evidencia de acceso no autorizado mediante cuentas privilegiadas.
- Ocurrencias anómalas que no están relacionadas con la operación normal de ninguna aplicación específica.
- Transmisiones de paquetes que tengan como origen al servidor y que no formen parte de la operación y/o administración normal y justificada.
- Alteración o modificación de la información contenida en el servidor sin razón justificada al sistema operativo, programas, paquetes, software, bases de datos, información o datos que formen parte de los elementos de administración, operación o mantenimiento del mismo.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.4 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto. Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de términos

En proceso.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
Eduardo José Herrerías López Director *General de Tecnologías e Innovación Digital.*	Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: Ana Laura Ortega Aguilar Jefa de la Unidad de Planeación y Control de TIC´s Dirección de Servicios Tecnológicos - DGTID.	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

CONTROLES CRIPTOGRÁFICOS

Referencia ISO 27001:2005. A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información. A.12.3 Controles Criptográficos

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.12.3 A.12.3.1	Controles Criptográficos Política de uso de los controles criptográficos	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Controles Criptográficos

Objetivo

Establecer, incorporar y mantener la seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de información de la DGTID, así como también, prevenir errores, pérdida, modificación o mal uso de la información, garantizando su seguridad.

1.0 Propósito

El propósito de esta política es establecer, incorporar y mantener la seguridad para la adquisición, desarrollo, procesamiento y mantenimiento de los sistemas de información de la DGTID, mismos que los Diseñadores, Desarrolladores y Administradores de los Sistemas y/o Servicios, de la Dirección de Servicios Tecnológicos de la DGTID, deberán incorporar y mantener dentro de sus actividades cotidianas, a fin de disminuir los riesgos a que están expuestos los sistemas de información de la APE y garantizar su seguridad.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

2.0 Ámbito de Aplicación

Esta política aplica para los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, aun cuando estos sean terceros prestadores al servicio a esta Dirección, equipos servidores propiedad y operados por o para La Administración Pública del Estado de Oaxaca, así como los servidores registrados bajo el dominio de red interna propiedad de la DGTID

Esta política aplica para los equipos de hardware y humano ubicados fuera de la red interna del uso y aprovechamiento de Tecnologías de la Información y que se encuentren por cualquier relación contractual bajo la administración de un Tercero.

3.0 Política

3.1 Descripción de Política

POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS

Se ha formulado e implementado una política para el uso de los controles criptográficos para proteger la información de la siguiente manera:

Para el Sistema de Gestión de Seguridad de la Información, la DGTID se asegura de encriptar los datos almacenados en dispositivos removibles, así como, de definir zonas de encriptación y controlar el acceso mediante uso de contraseñas, para proteger la confidencialidad, autenticidad o la integridad de la información por medios criptográficos, cumpliendo todos los acuerdos y reglamentos pertinentes según aplique (información del certificado).

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.3 Monitoreo

Todos los eventos de seguridad relacionados a sistemas críticos o sensibles en la operación de para las Dependencias y Entidades del Estado, deben ser registrados en las bitácoras (logs) y auditados de la siguiente manera:

- Todas las bitácoras de seguridad deben mantenerse en línea por lo menos una semana.

Los eventos e incidentes de seguridad deben reportarse a la Dirección General de Tecnologías e Innovación Digital del uso y aprovechamiento de Tecnologías de la Información, quien será el único responsable de revisar las bitácoras y reportar los incidentes correspondientes. Las medidas correctivas serán determinadas de acuerdo con el riesgo y severidad de las mismas.

3.4 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto. Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de términos

En Proceso.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López Director *General* *Dirección General de Tecnologías e Innovación Digital*	Ing. Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

SEGURIDAD DE LOS ARCHIVOS DE SISTEMA

Referencia ISO 27001:2005. A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información. A.12.4 Seguridad de los archivos de sistema

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.12.4 A.12.4.2	Seguridad de los archivos de sistema Protección de los datos de prueba del sistema	2	2.0	En proceso
A.12.5 A.12.5.1	Seguridad en los procesos de desarrollo y soporte Procedimientos de control de cambios	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Seguridad de los archivos de sistema y Seguridad en los procesos de desarrollo y soporte

Objetivo

Establecer, incorporar y mantener la seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de información de la DGTID, así como también, prevenir errores, pérdida, modificación o mal uso de la información, garantizando su seguridad.

1.0 Propósito

El propósito de esta política es establecer, incorporar y mantener la seguridad para la adquisición, desarrollo, procesamiento y mantenimiento de los sistemas de información de la DGTID, mismos que los Diseñadores, Desarrolladores y Administradores de los Sistemas y/o Servicios, de la Dirección de Servicios Tecnológicos de la DGTID, deberán incorporar y

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

mantener dentro de sus actividades cotidianas, a fin de disminuir los riesgos a que están expuestos los sistemas de información de la APE y garantizar su seguridad.

2.0 Ámbito de Aplicación

Esta política aplica para los Administradores de los Sistemas y/o Servicios de la Dirección General de Tecnologías e Innovación Digital, aun cuando estos sean terceros prestadores al servicio a esta Dirección, equipos servidores propiedad y operados por o para La Administración Pública del Estado de Oaxaca, así como los servidores registrados bajo el dominio de red interna propiedad de la DGTID

Esta política aplica para los equipos de hardware ubicados fuera de la red interna y que se encuentren por cualquier relación contractual bajo la administración de un Tercero.

3.0 Política

3.1 Descripción de Política

SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

- Se deberá garantizar que los desarrollos y actividades de soporte a los sistemas de información, se lleven a cabo de manera segura, con un control de acceso adecuado.

PROTECCIÓN DE DATOS DE PRUEBA DEL SISTEMA

- La Dirección General de Tecnologías e Innovación Digital debe realizar pruebas (funcionales, de estrés, interfaces, y de motores de operación) una vez terminada la fase de desarrollo. Las pruebas las debe realizar personal independiente al grupo de desarrolladores. Se debe generar un plan de pruebas y documentación con los resultados de las pruebas.

- Posteriormente se deben realizar pruebas funcionales con los usuarios. Se debe generar un reporte de las pruebas realizadas y los resultados obtenidos. El dueño del activo debe certificar las pruebas y autorizar la liberación a producción.

- No se deben utilizar datos de producción para realizar las pruebas. Se deben implementar controles para prevenir que la información despersonalizada sea distribuida fuera del ambiente de pruebas o regresada a producción.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

LIBERACIÓN Y PRODUCCIÓN

- La liberación de aplicaciones a producción se debe realizar por personal independiente al grupo de desarrollo y preferentemente independiente al grupo de pruebas.

- Está prohibida la migración directa de desarrollo a producción.

- Antes de liberar nuevas aplicaciones a producción el dueño debe clasificarlas.

DESARROLLOS A SOLICITUD A TERCEROS

- Cuando el desarrollo o mantenimiento de aplicaciones sea realizado por terceros prestadores de servicios de la Dirección General de Tecnologías e Innovación Digital, se deberá cumplir adicionalmente con los siguientes requerimientos:

    - Definir la propiedad del código fuente y derechos de autor a favor de la Dirección General de Tecnologías e Innovación Digital.
    - Definir los requerimientos de calidad del código.
    - Definir los derechos de la Dirección General de Tecnologías e Innovación Digital para auditar la calidad y exactitud del código.
    - Definir los criterios de aceptación del código.
    - Definir los tipos de pruebas requeridos (funcionales, estrés, interfaces, etc.).
    - Plazo de Garantía del Servicio y Soporte.

ENTRENAMIENTO

- Se debe proveer entrenamiento a los usuarios, así como generar manuales de usuario y operación, y según sea el caso el manual de DRP correspondiente.

RESTRICCIONES PARA LOS DESARROLLADORES

- Está prohibido que los desarrolladores realicen las siguientes actividades:

    - Pruebas de aceptación del software que desarrollaron.
    - Realizar las funciones de bibliotecario.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Migrar sistemas nuevos o modificados al ambiente de producción.
- Acceder al ambiente de producción.

- Únicamente en caso de emergencias y por autorización del Oficial de Seguridad de la Información podrán acceder los desarrolladores al ambiente de producción. Se debe documentar y justificar dicho acceso. Se debe generar una cuenta de acceso temporal la cual debe ser monitoreada y eliminada una vez que haya terminado la contingencia. Se debe entregar un reporte del uso de la cuenta al Administrador de la Información. Los cambios al software para reparar un problema se deben realizar en el ambiente de desarrollo.

CONTROL DE HERRAMIENTAS DE DESARROLLO

- El software de desarrollo (Ej. Compiladores) únicamente debe estar disponible para personal autorizado encargado del desarrollo de aplicaciones. No debe existir software de desarrollo en el ambiente de pruebas o producción.

SEPARACIÓN DE AMBIENTES

- El ambiente de desarrollo debe estar separado del ambiente de pruebas y producción. De preferencia la separación de ambientes debe ser física.

CONTROL DE VERSIONES

- Se deben proveer herramientas y procedimientos para el control de versiones de software.
- El Administrador en jefe de desarrollo (o el bibliotecario), debe ser responsable de almacenar y entregar al Oficial de Seguridad de la Información el Código Fuente. El personal encargado con la función de bibliotecario debe llevar un registro y control del código fuente. Se debe garantizar que la versión del código fuente sea puesta en producción.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

PROCEDIMIENTOS CONTROL DE CAMBIOS

- Se debe llevar un procedimiento para llevar el registro y control de los cambios realizados.
- Los cambios deben estar aprobados por el dueño del activo antes de su desarrollo y deberán contar con la aprobación de la Dirección de Servicios Tecnológicos, antes de su liberación a producción. Los cambios mayores o de alto impacto deben ser autorizados además por un Comité de Cambios de la DGTID.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Monitoreo

Todos los eventos de seguridad relacionados a sistemas críticos o sensibles en la operación de para las Dependencias y Entidades del Estado, deben ser registrados en las bitácoras (logs) y auditados de la siguiente manera:

- Todas las bitácoras de seguridad deben mantenerse en línea por lo menos una semana.

Los eventos e incidentes de seguridad deben reportarse a la Dirección de Servicios Tecnológicos, quien será el único responsable de revisar las bitácoras y reportar los incidentes correspondientes. Las medidas correctivas serán determinadas de acuerdo con el riesgo y severidad de estas.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.4 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto. Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de términos

En Proceso

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

NOTIFICACIÓN DE EVENTOS Y PUNTOS DÉBILES DE LA SEGURIDAD DE LA INFORMACIÓN.

Referencia ISO 27001:2005. A.13. Gestión de Incidentes en la Seguridad de la Información A.13.1 Notificación de Eventos y Puntos Débiles de la Seguridad de la Información.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.13.1. A.13.1.1 A.13.1.2	Notificación de Eventos y Puntos Débiles de la Seguridad de la Información Notificación de los eventos de seguridad de la información Notificación de puntos débiles de la seguridad	2	2.0	En proceso
A.13.2 A.13.2.2	Gestión de incidentes de seguridad de la información y mejoras Aprendizaje de los incidentes de	2	2.0	En proceso

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

	seguridad de la información			
Vigencia a partir de:	**Marzo 2019**			

Título de la Política

Gestión de Incidentes de Seguridad de la Información

Objetivo

Establecer los mecanismos y procedimientos necesarios para notificar los eventos y puntos débiles de la seguridad de la información de la DGTID, de tal forma que se cuente con las posibilidades de corregir oportunamente los problemas que se presenten y reanudar los servicios en el menor tiempo posible.

1.0 Propósito

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información, un impedimento en la operación normal de las redes, sistemas o recursos informáticos, o una violación a la Política de Seguridad de la Información.

El propósito es minimizar los efectos de estos incidentes de seguridad en la Administración Pública del Estado (sean éstas resultado de pérdida del servicio, equipo o medios, mal funcionamiento o sobre carga del sistema, errores humanos, etc.), resolverlas y reanudar los servicios en operación normal en el menor tiempo posible, así como también, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes.

2.0 Ámbito de Aplicación

Esta política se aplica a todos los dominios tecnológicos en administración y custodia de la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.0 Política

3.1 Descripción de Política

- La Jefatura de Unidad de Planeación y Control de TICS, deberá concientizar al personal de la importancia de notificar los incidentes de seguridad, permitiendo con ello responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades, minimizando la pérdida de información y la interrupción de los servicios.

- La Jefatura de Unidad de Planeación y Control de TICS, deberá ser el punto central de comunicación, tanto para recibir los informes de incidentes de seguridad, como para difundir información esencial sobre los incidentes quien deba hacerlo.

- La Jefatura de Unidad de Planeación y Control de TICS, deberá solicitar al personal que notifique algún evento y/o punto débil de seguridad, documentar y catalogar dichos incidentes (Accesos no autorizados, Código Malicioso, mal uso de los recursos tecnológicos, falla en la infraestructura tecnológica y/o en los servicios, etc.).

- La Jefatura de Unidad de Planeación y Control de TICS, deberá aumentar el nivel de conciencia con respecto a la seguridad dentro de la Dirección General de Tecnologías e Innovación Digital para ayudar a evitar que se den incidentes que lleguen a perjudicar la funcionalidad del Estado de Oaxaca.

- La Jefatura de Unidad de Planeación y Control de TICS, deberá posibilitar la auditoría de sistemas y redes mediante procesos como la evaluación de vulnerabilidades y pruebas de penetración.

- Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas a la Dirección General de Tecnologías e Innovación Digital.

- Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

- La notificación del evento de seguridad deberá contener los siguientes datos:

    - Describir la situación inicial del evento
    - Identificar el evento y su gravedad.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Notificar el evento al Oficial de Seguridad
- Tratar de contener el daño y minimizar el riesgo
- Notificar a los involucrados para resolver el evento

Una vez resuelto deberá documentarse, efectuarse el reporte respectivo y entregarse al Oficial de Seguridad.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefe de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado. Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

5.0 Definición de Términos

Término	***Definición***
Notificación	Comunicar, informar de forma oficial y con las debidas formalidades.
Evento de Seguridad	Incidente que atente contra la Confidencialidad, Integridad y Disponibilidad de la información y los recursos tecnológicos.
Puntos Débiles	Vulnerabilidades, medidas de cuán susceptible es un bien expuesto a ser afectado por un fenómeno perturbador.

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

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

Referencia ISO 27001:2005. A.14. Gestión de la Continuidad del Negocio A.14.1 Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.14.1. A.14.1.1 A.14.1.2	Aspectos de seguridad de la información en la gestión de continuidad del negocio. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio Continuidad del negocio y evaluación de riesgos	2	2.0	En proceso
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Gestión de la Continuidad Operativa.

Objetivo

Establecer los aspectos en la gestión de continuidad operativa, minimizando los efectos de las posibles interrupciones de las actividades y servicios de los sistemas informáticos e infraestructura de TI, asegurando su reanudación oportuna.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

1.0 Propósito

Minimizar los efectos ante posibles interrupciones de las actividades normales de servicios de la Infraestructura Tecnológica (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

2.0 Ámbito de Aplicación

Esta política aplica para todos los sistemas críticos identificados como esenciales para la provisión de servicios al público, así como de los activos de Tecnología de la Información (sistemas operativos, bases de datos, aplicaciones y dispositivos de red) que administra la DGTID.

3.0 Política

3.1 Descripción de Política

INCLUSIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GNC

- La Jefatura de la Unidad de Planeación y Control de TIC´s, será responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad operativa de los sistemas críticos del Estado.

- El plan de recuperación debe mantener al personal preparado previamente a que ocurra un desastre cubriendo todas las incidencias, además debe contener claramente lo siguiente:

    - Procedimientos de evacuación.
    - Procedimientos para declarar desastres.
    - Circunstancias en que se debe declarar desastre.
    - Identificación de responsabilidades en el plan.
    - Identificación de personas y funciones en el plan.
    - Identificación de información de los contratos.
    - Explicación paso a paso de la recuperación.
    - Identificación de recursos necesarios.
    - Aplicación paso por paso de la etapa de recuperación.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

- Se deberá garantizar la seguridad del personal y la protección de los medios de procesamiento de la información.

- El Plan de Recuperación (DRP) debe contar con las siguientes etapas:

  - Activación del plan: notificación del plan, detección y determinación del posible daño
  - Reanudación: restauración temporal de las operaciones y recuperación del daño producido al sistema original.
  - Recuperación: restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

- La Jefatura de la Unidad de Planeación y Control de TIC´s, debe asegurar la coordinación con el personal de la DGTID y los contactos externos que participarán en las estrategias de planificación de contingencias.

- La Dirección General o la Dirección de Servicios Tecnológicos, deberán tomar la decisión de activar el plan de recuperación, coordinando las actividades de recuperación y las acciones para regresar a la operación normal una vez que hayan sido restablecidas las actividades críticas.

- Dentro del plan de recuperación, tanto los propietarios de la información como la Dirección de Servicios Tecnológicos deberán:

  - Identificar las amenazas que puedan ocasionar interrupciones de los procesos críticos de la DGTID.
  - Evaluar los riesgos para determinar el impacto de dichas interrupciones.
  - Identificar los controles preventivos.
  - Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la DGTID.
  - Analizar las consecuencias de la interrupción del servicio y tomar las medidas necesarias para prevenir situaciones similares.

CONTINUIDAD DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

- El Análisis de Riesgos (Análisis de Impacto en el Negocio (BIA)) de la DIRECCIÓN DE SERVICIOS TECNOLÓGICOS identifica los requerimientos de seguridad (inventario de

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

activos, vulnerabilidades, amenazas, probabilidad de ocurrencia de las amenazas, impacto estimado, etc.), así mismo el dueño del activo y el Oficial de Seguridad de la Información, deberán evaluar los riesgos de cada activo.

- El plan de recuperación (DRP), debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.

- El plan de recuperación debe identificar los controles preventivos, como son los sistemas de supresión de fuego, detectores de humo y fuego, los registros no electrónicos vitales, etc.

3.2 Matriz de Responsabilidades

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

3.3 Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado. Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.

Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca,

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Plan de Recuperación (DRP)	Conjunto de procedimientos para lograr la recuperación en caso de algún desastre o eventualidad (DRP: Disaster Recovery Plannig). Forma parte del Plan de Continuidad del Negocio (BCP: Business Continuity Plannig).

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
L.I. Eduardo José Herrerías López *Director General* *Dirección General de Tecnologías e Innovación Digital*	*Ing. Patricia Elena García Herrera* *Directora de Servicios Tecnológicos* *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: *M.T.I. Ana Laura Ortega Aguilar* *Jefa de la Unidad de Planeación y Control de TIC´s* *Dirección de Servicios Tecnológicos - DGTID*	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

ADMINISTRACIÓN Y GESTIÓN DE RIESGOS

Referencia ISO 27001:2005. A.14. Gestión de la Continuidad del Negocio A.14.1 Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Control	***Área de aplicación***	***Número de actualización***	***Versión***	***Estado actual del procedimiento programado, en proceso, concluido***
A.14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	2	2.0	Programado
A.14.1.4	Marco de referencia para la planificación de la continuidad del negocio			
A.14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad			
Vigencia a partir de:		**Marzo 2019**		

Título de la Política

Administración y Gestión de Riesgos de TIC's

Objetivo

La presente política tiene como objetivo establecer los criterios mínimos para la identificación, administración, gestión y control de los riesgos asociados a TI, a fin de

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

contribuir positivamente a la seguridad, disponibilidad, y eficiencia del uso de dicha tecnología por las áreas de negocio involucradas en proveer de servicios a la ciudadanía.

1.0 Propósito

Minimizar los efectos de las posibles interrupciones de las actividades normales de las unidades administrativas y de negocio de la APE, protegiendo los procesos críticos de operación de TI mediante una combinación de controles preventivos y acciones de recuperación.

2.0 Ámbito de Aplicación

Esta política aplica para todos los sistemas de misión crítica identificados en las unidades administrativas y de servicio, así como los activos de Tecnología de la Información (sistemas operativos, bases de datos, aplicaciones y dispositivos de red) de la DGTID.

3.0 Política

3.1 Descripción de Política

Todos los sistemas en producción deberán ser **evaluados periódicamente** por la Dirección de Servicios Tecnológicos, para determinar el mínimo conjunto de controles requeridos para reducir y mantener los riesgos a un nivel aceptable de tal forma que puedan ser priorizados por riesgo.

Por lo que deberá efectuarse un análisis de riesgos que identifique:

- Activo
- Vulnerabilidades
- Amenazas
- Probabilidad de ocurrencia de las amenazas
- Impacto estimado
- Regulaciones que deben cumplirse

La auditoría de los procesos de gestión de riesgos deberá llevarse a cabo al menos una vez al año.

La administración de riesgos deberá evaluar y administrar los riesgos, asumiendo que toda la Organización debe estar consciente que siempre existen riesgos residuales con los que tiene que llevarse a cabo el trabajo, de tal forma que el impacto que conlleve sea el menor posible.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Con la finalidad de garantizar el mínimo **nivel de riesgo**, se deberá **concienciar al personal** sobre la necesidad de cumplir y respetar las políticas de seguridad de la información y los estándares, mismos que pretenden prever el sabotaje, el terrorismo, el fraude, los errores, las omisiones, las interrupciones del servicio, el robo de equipos y la violación de la privacidad, entre otros, cubriendo las necesidades de la DGTID en materia de seguridad de la información.

PLANEACIÓN, ORGANIZACIÓN Y GESTIÓN

La Dirección General de Tecnologías e Innovación Digital ha definido los objetivos, lineamientos y políticas para administrar de manera adecuada y prudente los riesgos operacionales y de tecnología de la información, incidiendo positivamente en los procesos críticos asociados a dicho riesgo.

Será su responsabilidad el velar por el cumplimiento de las referidas políticas y procedimientos, así mismo de las disposiciones contenidas en la presente política. Para tales efectos se deberá considerar lo establecido en las mejores prácticas Internacionales para control y seguridad de la TI tales como COBIT e ISO/IEC 27001:2005, además de las guías sobre la materia que se consideren necesarias de acuerdo con la industria y sector.

Los objetivos, lineamientos y políticas antes referidos, se deberán revisar con una frecuencia cuando menos anualmente.

Corresponderá a la Jefatura de la Unidad de Planeación y Control de TIC´s, la implementación de las políticas y procedimientos generales establecidos por la Dirección General de Tecnologías e Innovación Digital en materia de Gestión del Riesgo.

ESTRUCTURA ORGANIZACIONAL Y PROCEDIMIENTOS

La Dirección General de Tecnologías e Innovación Digital deberá definir y mantener una estructura organizacional y procedimientos que le permita administrar adecuadamente los riesgos asociados a la TI, consistente con su tamaño y naturaleza, así como con la complejidad de las operaciones que realizan.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

La Dirección de Servicios Tecnológicos, deberá implementar una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico.

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá asegurarse que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos.

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá definir e implementar procedimientos relevantes para controlar las actividades de consultores y demás personal externo contratado por la DGTID o las unidades de negocio, para asegurar la protección de los activos de información de la organización.

PLANEACIÓN ESTRATÉGICA Y OPERATIVA

La Dirección General de Tecnologías e Innovación Digital será responsable de desarrollar planes de largo y corto plazo de TI que apoyen el logro de la misión y las metas generales del APE.

La Dirección de Servicios Tecnológicos deberá crear y actualizar regularmente un Plan de Infraestructura Tecnológica de acuerdo con las mejores prácticas internacionales de la industria y en concordancia al PED 2016-2022 y con los planes a largo y corto plazo de la DGTID.

Dicho plan deberá abarcar aspectos tales como arquitectura tecnológica y soporte al cliente, así como estrategias de reingeniería y diseños de nuevas estrategias de operación a favor de los derechohabientes.

Este plan deberá ser evaluado sistemáticamente en cuanto a aspectos de contingencia (como redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura). De igual manera deberá establecerse un Marco de Gestión del Riesgo y Dominios Tecnológicos referente a la administración de la infraestructura de tecnología de la DGTID.

ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO

Las unidades operaciones de la Dirección General de Tecnologías e Innovación Digital, deberán administrar apropiadamente los riesgos asociados a TI, de tal modo que se

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

minimice la posibilidad de pérdidas en la provisión de servicios, derivadas del uso de inadecuados procedimientos de trabajo y tecnologías relacionadas a ellos, que pueden afectar el desarrollo de las operaciones y servicios que realiza la APE al atentar contra la confidencialidad, integridad y disponibilidad de la información, ya sea de usuarios o de los usuarios de la Dirección General de Tecnologías e Innovación Digital.

Las unidades operacionales de la Dirección General de Tecnologías e Innovación Digital deberán considerar los riesgos vinculados a las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de sus operaciones y servicios, así como la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, las fallas en la adecuación a los objetivos del negocio, entre otros aspectos.

La administración del riesgo tecnológico debe permitir el adecuado cumplimiento de los siguientes criterios de control interno:

- Eficacia. La información debe ser relevante y pertinente para los objetivos de la APE y ser entregada en una forma adecuada y oportuna conforme las necesidades de los diferentes niveles de decisión y operación en la provisión de los servicios de la Dirección General de Tecnologías e Innovación Digital.

- Eficiencia. El proceso de la información debe realizarse mediante una óptima utilización de los recursos asignados a la provisión de servicios.
- Confidencialidad. La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados dentro de cada proyecto.
- Integridad. La información debe ser completa, exacta y válida.

- Disponibilidad. La información debe estar disponible en tiempo y en forma organizada para los usuarios autorizados cuando sea requerida.

- Cumplimiento Normativo. La información debe cumplir con los criterios y estándares internos de la Dirección General de Tecnologías e Innovación Digital, las regulaciones definidas externamente por el marco legal aplicable y las correspondientes entidades reguladoras, así como los contenidos de los SOW.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

ADMINISTRACIÓN DE NUEVOS PROYECTOS

Se deberá establecer un marco referencial general para la administración de proyectos que defina el alcance, límites y metodología de administración de proyectos. Dicha metodología estará alineada al estándar definido por el Program Manager Institute (PMI), debiendo poner atención en seguir al pie de la letra, el cubrir la asignación de responsabilidades, bases para asignar al equipo de trabajo y sus responsabilidades, participación de las áreas usuarias, determinación de tareas, presupuestos de tiempo y recursos, avances, criterios y puntos de revisión y aprobación de las revisiones post-implementación.

ADMINISTRACIÓN DE LAS OPERACIONES Y COMUNICACIONES

Se deberán establecer medidas de administración de las operaciones y comunicaciones que entre otros aspectos contendrán lo siguiente:

- Control sobre los cambios en el ambiente operativo, que incluye cambios en la operación, servicios o productos, las instalaciones de procesamiento y los procedimientos.
- Control sobre los cambios en la provisión de servicios o entregables.
- Separación de funciones para reducir el riesgo de error o “fraude”.
- Separación del ambiente de producción y de desarrollo.
- Controles preventivos y de detección sobre código malicioso, uso de software de procedencia dudosa, virus y otros similares.
- Seguridad sobre la red de medios de almacenamiento y documentación de sistemas.
- Seguridad sobre correo electrónico.

ADMINISTRACIÓN Y MONITOREO DE LOS NIVELES DE SERVICIO

Se deberán establecer estrategias y procedimientos de trabajo orientados a garantizar a los usuarios internos, derechohabientes y acreditados de la Dirección General de Tecnologías e Innovación Digital, los niveles de disponibilidad y respuesta de los servicios soportados en TI, prestados y/o recibidos, ya sean brindados por el APE o por Terceros.

ESTÁNDARES DE DESARROLLO Y MANTENIMIENTO

Se deberán definir e implementar estándares de sistemas de información y adoptar una metodología de ciclo de vida del sistema que rija el proceso de análisis, desarrollo,

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

implementación y mantenimiento de sistemas computarizados y tecnología afín, debiendo incorporar estándares para la documentación de procesos y programas, requerimientos de pruebas, verificación de software; definiendo condiciones bajo las cuales deberán conducirse las pruebas pilotos o en paralelo de los sistemas nuevos y/o actuales y revisiones post-implementación, además de los criterios de certificación, aceptación y aprobación por parte del usuario.

ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES

Se deberá definir e implementar un sistema de administración de problemas, incidentes y errores para asegurar que los eventos operacionales que no formen parte de la operación normal sean registrados, documentados, analizados y resueltos, debiendo conservarse por tiempo indefinido para utilizarlos como gestión del conocimiento y facilite la solución de problemas similares a futuro.

DOCUMENTACIÓN

Se deberá elaborar y mantener actualizada, al menos la siguiente documentación:

- Procesos de Operación: operación de los procesos de servicios, procesos de recuperación de datos y archivos, procesos de copias y resguardo de datos, seguridad física y lógica, administración de la red de telecomunicaciones, procedimientos para la puesta en marcha de servicios, tratamiento de los requerimientos de usuarios, manuales técnicos y de usuario, procedimientos de transferencia electrónica de datos, procesos especiales de cierre de proyectos y servicios.

- Equipamiento de infraestructura tecnológica: diagramas y distribución física de las instalaciones, inventario de “hardware” y “software”, diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos, etc.

Esta información comprende tanto al Edificio Principal del uso y aprovechamiento de Tecnologías de la Información, Edificio de Tecnología de la Información (Anexo) de la Dirección General de Tecnologías e Innovación Digital, Departamentos de Vivienda o Gerencias Regionales, Enlaces de Información con Proveedores y Centro de Datos Alterno.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

GESTIÓN DE RELACIONES CON TERCEROS

Cuando ciertas funciones o procesos puedan ser objeto de una subcontratación, La Administración Pública del Estado de Oaxaca deberá proceder conforme la norma que regula la materia.

MANTENIMIENTO DE LOS REGISTROS ADECUADOS

Que permitan verificar el cumplimiento de las políticas, procedimientos, estándares, lineamientos y otros definidos por la Dirección, así como mantener pistas de auditoría adecuadas.

ASPECTOS DE LA SEGURIDAD DE INFORMACIÓN

Para la administración de la seguridad de la información, las unidades organizacionales de la DGTID deberán tomar en consideración los siguientes aspectos:

Seguridad Lógica

Se deberá implementar y seguir la política para el control de accesos, que incluya los criterios para la concesión, administración y revocación de los accesos a los sistemas de la Dirección General de Tecnologías e Innovación Digital, redes y sistemas operativos, así como los derechos y atributos que se confieren a bases de datos (aplicados tanto al interior como al exterior negocio).

- Procedimientos formales para la concesión, administración y revocación de derechos, perfiles y usuarios. Deberán efectuarse revisiones periódicas sobre los derechos concedidos a los usuarios.

- Políticas de uso de usuarios genéricos y control de no repudiación de responsabilidades. Los usuarios deberán contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.

- Seguimiento sobre el acceso, uso de los sistemas y otras instalaciones físicas para detectar actividades no autorizadas.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Seguridad de Personal

La Dirección General de Tecnologías e Innovación Digital deberá definir procedimientos para reducir los riesgos asociados al error humano, robo, fraude o mal uso de activos, vinculados al riesgo de TI. Al establecer estos procedimientos deberá tomarse en consideración, entre otros aspectos, la adecuada definición de roles y responsabilidades establecidos sobre la información y su procesamiento, verificación de antecedentes, políticas de rotación y vacaciones, control cruzado y compartido de operaciones sensitivas, y entrenamiento constante.

Seguridad Física y Ambiental

La Dirección General de Tecnologías e Innovación Digital deberá definir adecuados controles físicos y ambientales al acceso, daño o manejo de información en dependencia del nivel de protección requerido. El alcance incluirá las instalaciones físicas, áreas de trabajo, equipamiento, cableado, entre otros bienes físicos susceptibles a riesgos de seguridad.

Clasificación de Seguridad

La DIRECCIÓN DE SERVICIOS TECNOLÓGICOS deberá realizar un inventario periódico de activos físicos y lógicos asociados a la tecnología de la información que tenga por objetivo proveer la base para una posterior clasificación de seguridad de acuerdo al estándar de clasificación de activos, dictada por la Dirección General de Tecnologías e Innovación Digital. Esta clasificación debe indicar el nivel de criticidad y/o riesgo existente.

PLANES DE CONTINGENCIA Y RECUPERACIÓN DE DESASTRES

Procedimientos de Respaldo

La Dirección General de Tecnologías e Innovación Digital deberá establecer procedimientos de respaldos regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas deben ser probadas periódicamente para verificar su efectividad y ser coherentes con lo requerido en el Plan de Contingencia.

El APE deberá conservar la información de respaldo y los procedimientos de restauración, debiendo resguardar con una frecuencia razonable una copia de los mismos en una

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento de datos o en sus instalaciones.

Se deberá seguir conforme a la política de respaldos, el mantenimiento de data histórica debe tomar en cuenta los estudios de criticidad de los procesos e información, los tiempos objetivos de recuperación y restauración, así como el tiempo de resguardo de registros; considerando las disposiciones legales vigentes o bien los requerimientos de protección de la información de la Dirección General de Tecnologías e Innovación Digital.

Diseño e Implementación del Plan de Contingencia

La Dirección General de Tecnologías e Innovación Digital debe establecer un proceso de planeación de contingencia que provea los procedimientos y la capacidad de dar continuidad al soporte general y a las aplicaciones críticas durante la contingencia y recuperación de un desastre, considerando una evaluación de riesgos asociados a la seguridad de la información y el desarrollo de sub-planes específicos para proteger, mantener y recuperar los procesos críticos de negocios a la menor brevedad posible.

El proceso de planeación de contingencia debe incluir cuando menos las siguientes etapas:

- Creación de una política de contingencia del negocio y de recuperación de desastres.
- Análisis de impacto de negocio.
- Clasificación de las operaciones y análisis de criticidad.
- Análisis de tiempo mínimo de respuesta a los procesos críticos.
- Definición de las estrategias de recuperación.
- Desarrollo el plan de contingencia de negocios y procedimientos de recuperación de desastres.
- Programa de entrenamiento, divulgación y concientización de los planes.
- Prueba e implementación.
- Monitoreo y actualización continua de los planes.

El Plan de Recuperación de Desastres estará dirigido a la ocurrencia de catástrofes que no permitan la utilización normal de las instalaciones de procesamiento de la Dirección General de Tecnologías e Innovación Digital por períodos extensos.

Este plan debe permitir la restitución de los sistemas, aplicativos críticos y actividades de procesamiento de información en un sitio alterno bajo condiciones de operación adecuadas. El contenido de este plan puede coincidir en parte con el del plan de

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

contingencia, sin embargo, su alcance es menor ya que no debe abarcar interrupciones menores que no requieran reubicación.

Requerimientos de Información
Evaluación Anual del Riesgo Tecnológico

La Jefatura de la Unidad de Planeación y Control de TIC's, deberá realizar al menos una vez al año la evaluación del riesgo tecnológico que enfrenta el APE por proceso o unidad de negocio.

El informe de dicha evaluación debe ser presentado a la Dirección General de Tecnologías e Innovación Digital cuando este lo requiera. El informe deberá contemplar por lo menos los siguientes aspectos:

- Metodología empleada para la administración del riesgo tecnológico y su engranaje dentro del marco de la administración del riesgo operacional e integral de la Dirección General de Tecnologías e Innovación Digital.
- Identificación del riesgo tecnológico por proceso o unidad de negocio y apoyo.
- Medidas adoptadas para administrar los riesgos tecnológicos, materiales identificados y plazos para su aplicación.
- Dueños de proceso o procesos responsables de las actividades de control de riesgos identificadas.
- Plan de actividades en lo referente a la administración del riesgo tecnológico.

Informes y Reportes

La Jefatura de la Unidad de Planeación y Control de TIC´s, deberá elaborar la estrategia de información y reportes para la Dirección General de Tecnologías e Innovación Digital, así como la documentación que servirá de base de conocimiento que deberá resguardarse en su repositorio correspondiente.

PRUEBAS, MANTENIMIENTO Y REEVALUACIÓN DE PLANES DE CONTINUIDAD

- El plan de recuperación, debe considerar efectuar pruebas y/o simulacros tanto calendarizados como improvisados, en las instalaciones alternas para que las áreas de servicio puedan continuar las operaciones y las actividades críticas en caso de alguna

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

interrupción o eventualidad, para asegurar la efectividad del mismo (en tiempo y forma).

- El procedimiento, la frecuencia y profundidad de dichas pruebas deberá responder a la evaluación formal y prudente que sobre dicho riesgo realice cada unidad de negocio, debiendo realizar al menos una prueba al año.

- El cronograma de pruebas, los resultados de pruebas efectuadas y el control de cambios sobre el plan derivado de las mismas deben ser formalmente documentados y estar disponibles para cuando se requiera.

- Debe garantizarse que el plan de recuperación sea conocido y esté disponible en caso de contingencia o eventualidad.

- Se deberá capacitar al personal involucrado en cuanto al procedimiento a seguir en caso de contingencia o eventualidad.

- Se deben realizar revisiones periódicas para verificar la completitud y difusión del Plan de recuperación, así como para revisar los resultados de las pruebas.
- El plan de recuperación debe revisarse y probarse por lo menos una vez al año; el sitio alterno de recuperación debe revisarse semestralmente, la información de los contactos del personal clave y del directorio en caso de eventualidades, debe revisarse por lo menos semestralmente.

1.1 Matriz de Responsabilidad

Autorización:	Dirección General de Tecnologías e Innovación Digital / Dirección de Servicios Tecnológicos de la DGTID
Revisión	Jefatura de la Unidad de Planeación y Control de TIC´s de la Dirección de Servicios Tecnológicos
Administración y ejecución:	Personal de la Dirección General de Tecnologías e Innovación Digital y Dirección de Servicios Tecnológicos
Cumplimiento:	Todo el personal perteneciente la Administración Pública del Estado, usuarios y proveedores.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

3.3. Revisiones y Auditorías

Las auditorías serán realizadas en intervalos o periodos regulares por personal autorizado para tal efecto.
Las auditorías serán coordinadas por un grupo interno en concordancia con la Política de auditoría. El personal que realice los procesos de auditoría deberá presentar los resultados al grupo de trabajo responsable para sus correcciones o justificaciones.
Todos los esfuerzos de los procesos de auditorías se realizarán con el único y exclusivo objetivo de prevenir daños, riesgos o fallas en los sistemas o servicios de información.

4.0 Sanciones y Observaciones

Cualquier empleado de la APE que se encuentre en plena violación de los criterios establecidos por esta política puede ser sujeto de sanciones disciplinarias determinadas por el área de Recursos Humanos de la Secretaría de Administración del Poder Ejecutivo del Estado de Oaxaca, y con vista a la Secretaria de la Contraloría y Transparencia Gubernamental con base a las sanciones disciplinarias establecidas para tal efecto, en las Condiciones Generales de Trabajo que dicta la Secretaría de Administración, de acuerdo con el grado de severidad, riesgo y compromiso de la información o mal uso de la infraestructura tecnológica.

5.0 Definición de Términos

Término	***Definición***
Riesgo	Posibilidad de que se produzca un impacto determinado en un activo, en un sector o en toda la Organización. Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene y su probabilidad de ocurrencia.
	La evaluación del riesgo indica, el valor de la información, los riesgos a los cuales la información está supeditada y las vulnerabilidades asociadas con la forma actual de manejar la información.
Análisis de Impacto de Negocio	Etapa de la planeación de continuidad de negocio en la que se identifican los eventos que podrían tener un impacto sobre la continuidad de operaciones y su impacto financiero, humano y de reputación sobre la provisión y entrega de servicios de la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Base de Datos	Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados.
ISO/IEC 20000-1:2005)	Norma Internacional Certificable para la Seguridad de la Tecnología de la Información.
Control	Políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para procurar que los objetivos del negocio sean alcanzados y que eventos no deseables serán prevenidos, detectados y corregidos
Denegación de Servicios	Es un ataque a un servicio o recursos que provoca que este mismo sea inaccesible a sus usuarios.
Información	Activo Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
Muro de Fuego (Firewall)	Todo Hardware o Software y sus políticas que son utilizados como medida de control sobre el tráfico entrante y saliente entre una red y otra.
Objetivo de Control	Definición del propósito o resultado que se desea alcanzar mediante la implementación de controles específicos en una actividad de TI.
Plan de Contingencia	Documento donde se detallan los procedimientos por seguir en caso de una contingencia, con el fin de no afectar el funcionamiento normal de para las Dependencias y Entidades del Estado. Tiene como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.
Políticas	Conjunto de prácticas establecidas por la Junta Directiva de para las Dependencias y Entidades del Estado, por medio de las cuales se definen los cursos de acción a seguir por usuarios de TI de la DGTID.

Término	***Definición***
Procedimiento	Método o sistema estructurado para ejecutar instrucciones. Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de las cuales se asegura el cumplimiento de una función operativa.
Proceso Crítico	Proceso considerado indispensable para la continuidad de las operaciones y servicios DE LA DGTID, y cuya falta o ejecución deficiente puede tener un impacto financiero, social y de imagen significativo para la continuidad en la prestación de servicios.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

Término	***Definición***
Registros	Asentamiento manual o electrónico que provee información necesaria para identificar e investigar alguna actividad, problema o incidente.
Riesgo Operativo	Es el riesgo de pérdida debido a la inadecuada operación o fallos de los procesos, personal y los sistemas internos o bien a causa de acontecimientos externos.
Riesgos de Tecnología de Información	Perdida potencial por daño, interrupción, alteración o fallas derivadas del uso o dependencia en la TI que soporta los procesos críticos en la provisión de servicios.
Seguridad Lógica	Seguridad a nivel del Software para proteger los datos, procesos y sistemas
Tecnología de Información (TI)	Se traduce en hardware, software, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, servicios y organización de informática.
Unidades operacionales	Direcciones, Gerencias, Jefaturas y áreas de administración y soporte que forman parte de la estructura organizacional de la DGTID.

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512

6.0 Revisiones Históricas de la Política

Registrar la fecha y responsable de la actualización de la presente política.

Fecha de inicio de actualización: marzo 2019	Fecha de terminación de la actualización: marzo 2019
Responsable de la política: *Dirección General de Tecnologías e Innovación Digital*	Persona que ejecuta: Personal asignado a la Dirección de Servicios Tecnológicos
Fecha de la última actualización: marzo 2019	Fecha de la próxima actualización/revisión: diciembre 2020

Autoriza	Revisa
Eduardo José Herrerías López Director *General de Tecnologías e Innovación Digital.*	Patricia Elena García Herrera Directora de Servicios Tecnológicos *Dirección General de Tecnologías e Innovación Digital*
Responsable de Integración: Ana Laura Ortega Aguilar Jefa de la Unidad de Planeación y Control de TIC´s Dirección de Servicios Tecnológicos - DGTID.	

Carretera Internacional Oaxaca-Istmo Km 11.5
Ciudad Administrativa Benemérito de las Américas
Edificio 2, segundo nivel, Tlalixtac de Cabrera,
Oaxaca. C.P. 68270
Tel. Conmutador 01(951)5015000 ext.10512