POLÍTICAS DE USO DE EQUIPO DE CÓMPUTO, INTERNET Y RESGUARDO DE INFORMACIÓN

El presente documento tiene como objetivo establecer las políticas para la correcta utilización de los activos tecnológicos de información y comunicación de INDETEC, así como la información contenida en ellos.

12 DE JUNIO DE 2024

CONTENIDO

INTRODUCCIÓN

Es fundamental reconocer que las Tecnologías de Información y Comunicaciones (TIC) contribuyen a las mejores prácticas en el uso de instrumentos digitales, lo cual permite optimizar los recursos públicos y agilizar los servicios y/o procesos administrativos.

Para garantizar el mejor uso de los instrumentos digitales es de vital importancia el apego a la normatividad y preceptos establecidos en materia de las TIC, las cuales están diseñadas atendiendo a las políticas generales de la Estrategia Digital Nacional.

OBJETIVO

El presente documento, basado en el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTIC-SI)[1], tiene como objetivo promover el uso eficiente, transparente y eficaz de los activos tecnológicos de información y comunicación en el Instituto para el Desarrollo Técnico de las Haciendas Públicas.

Además, busca establecer políticas y disposiciones con el propósito de impulsar activamente el uso y aprovechamiento de la informática, el gobierno digital, las TIC, así como la seguridad de la información. Estas directrices serán de observancia obligatoria.

A lo largo de este instrumento se proporcionará orientación detallada para guiar al personal en la ejecución de sus operaciones diarias y el manejo de diversas herramientas tecnológicas. El objetivo es mejorar la productividad, reducir costos e identificar oportunidades de mejora. Para fomentar la conciencia y comprensión de las TIC en el Instituto se llevarán a cabo eventos, actividades de divulgación y otras formas de comunicación.

Adicionalmente, se implementarán estrategias de tecnología de la información que garanticen una supervisión adecuada de las herramientas y activos informáticos del Instituto. Asimismo, se asegurará que el Instituto cuente con sistemas apropiados para monitorear, controlar e informar sobre el cumplimiento de los requisitos de protección de datos, conforme a la legislación aplicable. Se desarrollará una estrategia formal de seguridad de datos que incluirá una evaluación y un enfoque basado en el riesgo, asegurando que esté alineada con las mejores prácticas establecidas.

ABREVIATURAS Y DEFINICIONES

La información de términos y abreviaturas de Tecnologías de la Información y Comunicación están contenidas en el documento de "Referencias y glosario de términos", ubicado en el Anexo 1.

---

[1] ACUERDO que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias (DOF 8/05/2014). Disponible en: https://www.gob.mx/cms/uploads/attachment/file/233743/MAAGTICSI_SFP2014.pdf

POLÍTICAS DE USO DE EQUIPO DE CÓMPUTO, INTERNET Y RESGUARDO DE LA INFORMACIÓN

A través de este documento se enuncian las políticas de uso en materia de los activos tecnológicos de información y comunicación de INDETEC en atención a la normatividad que le sea aplicable.

ALCANCE

Las presentes políticas están dirigidas al personal de INDETEC que tenga asignados activos de TIC para la ejecución y desarrollo de sus funciones.

USO DE ACTIVOS DE TIC

El Personal deberá firmar una CARTA RESGUARDO DE EQUIPO DE CÓMPUTO por los activos de TIC asignados, como la que se muestra en la Figura 1.

Figura 1. Muestra de Carta resguardo de equipo de cómputo

No. de Carta: **090_01**

Guadalajara, Jalisco., a 22 de noviembre de 2022

CARTA RESGUARDO DE EQUIPO DE CÓMPUTO

Asignado a: <Nombre de resguardarte>

Área de Adscripción: <Área del resguardarte>

Recibí del Instituto para el Desarrollo Técnico de las Haciendas Públicas, el equipo que se menciona a continuación:

Descripción de equipo:

Tipo	Características / Especificaciones						Número de Serie
Laptop	**Marca:** Lenovo **Modelo:** ThinkBook15 G2 ITL **RAM:** 8 GB | **Almacenamiento:** 512 GB SSD | **Procesador:** Intel Core _I5 1135G7 2.4 Ghz **S.O.:** Windows 11 PRO | **Color:** Plata | 15.6" | HDMI						MP29E40G
Cargador	Original Lenovo						-
Teclado	**Marca:**	-	**Modelo:**	-			-
Mouse	**Marca:**	-	**Modelo:**	-			-
Monitor/es	**Marca:**	-	**Modelo:**	-	**Pulgadas:**	-	-
	Marca:	-	**Modelo:**	-	**Pulgadas:**	-	-
Otro	**Marca:**	-	**Modelo:**	-			-
Elementos Adicionales	✓ Convertidor HDMI ✓ Mochila						

Salida del equipo para trabajo remoto: 23-11-2022

"Me comprometo a resguardar y dar un buen uso del equipo, utilizándolo únicamente para asuntos relacionados con mi actividad laboral en el INDETEC, a sabiendas de que, de no hacerlo, me haré acreedor a la sanción correspondiente: En caso de daño imputable a mi persona, me obligo a cubrir el costo de reparación del mismo; y en caso de pérdida, o extravío a la reposición del equipo o pago a valor en libros del mismo".

Bajo protesta de decir verdad, declaro que conozco y he leído las "Políticas de Uso de Computo, Internet y Resguardo de Información" y me comprometo a cumplirlas.

Cualquier perdida, robo o extravío de algún componente o hardware tiene que ser reportado al área de soporte técnico a la brevedad.

Responsable del Resguardo

Jefe Inmediato Superior

Adriana Mercado Gómez
Jefatura de Recursos Materiales

FTIC-0001

1. El personal asumirá la responsabilidad de salvaguardar con diligencia los activos de TIC que se le hayan asignado con el propósito exclusivo de llevar a cabo sus funciones, tareas y/o actividades, ya sea de manera presencial o remota. Se enfatiza que dichos activos no son transferibles y requieren un cuidado especial para garantizar su integridad y eficiencia en el desempeño de las labores encomendadas.
2. Una vez que se ha asignado un equipo de cómputo institucional, queda prohibido el uso de equipos personales para realizar actividades institucionales. Esto garantiza el buen funcionamiento de los recursos asignados y evita posibles conflictos de interés o pérdida de información confidencial. Además, promueve la responsabilidad en el uso de los recursos institucionales y contribuye a mantener la integridad y seguridad de los datos. Es importante respetar esta normativa para mantener un ambiente de trabajo profesional y eficiente.
3. Los activos de TIC en posesión del personal de INDETEC están previamente acondicionados y licenciados para llevar a cabo las funciones, tareas y actividades laborales asignadas por el Instituto. Se solicita expresamente al personal responsable de estos activos que se abstenga de instalar software, realizar modificaciones en la configuración, o cambiar/adicionar hardware en los equipos de INDETEC sin previa autorización.
4. En el caso de que sea necesario llevar a cabo cambios o adiciones, se requiere que el personal en resguardo de los activos envíe un correo electrónico al área de soporte interno, previa autorización de su jefe inmediato. Este correo debe detallar los cambios o adiciones necesarios y explicar cómo estos contribuirán a la ejecución efectiva de las tareas asignadas por el Instituto.
5. El personal de soporte interno tiene la exclusividad de realizar resguardos temporales con el fin de asignar equipos de uso común para llevar a cabo funciones, tareas y/o actividades institucionales. Estos préstamos se formalizarán mediante una bitácora que indique claramente la fecha de entrega acordada. Se subraya la preferencia de que estos equipos permanezcan en las instalaciones del instituto, salvo en casos excepcionales en los que se haya obtenido la autorización previa tanto del área de recursos materiales como del jefe directo del personal involucrado.
6. El Personal no podrá otorgar a personas ajenas a INDETEC, Activos de TIC en calidad de préstamo, con excepción de personas que requieran hacer efectivos sus derechos de acceso a información y protección de datos personales, a quienes, en el espacio autorizado, se le facilitará el equipo habilitado para ello.
7. El personal tiene prohibido reproducir, almacenar o transmitir copias no autorizadas de aplicaciones o información digital contenida en los activos de TIC asignados. Esta restricción garantiza la integridad y seguridad de los recursos tecnológicos, promoviendo un uso responsable y conforme a las políticas establecidas.

8. El personal almacenará únicamente información institucional en los equipos asignados. En casos que involucren datos personales, se concede al personal de soporte la autoridad para realizar la eliminación correspondiente de dicha información, asegurando que este procedimiento se lleve a cabo de manera adecuada y segura, con el propósito de evitar el almacenamiento de esta información personal en los medios institucionales.
9. El Personal no podrá modificar, alterar, ni copiar a otros medios la configuración del o los sistemas operativos, así como todos aquellos aplicativos instalados en los equipos de cómputo (a excepción del área de soporte interno).
10. No se utilizarán los activos de TIC de INDETEC para procesar, almacenar, descargar o enviar información que promuevan actos y propaganda política, religiosa, racista, étnica o social.
11. Queda estrictamente prohibido publicar o proporcionar datos personales de cualquier individuo, entidad pública o privada con la que exista alguna relación vinculada a INDETEC, a menos que se haya obtenido previamente la autorización correspondiente. Esta medida tiene como objetivo resguardar la información personal de quienes trabajan en el Instituto, priorizando así el uso de los dispositivos, plataformas y aplicaciones institucionales.
12. El personal no podrá comercializar ni difundir artículos, documentos o cualquier otro material o información que contenga el registro de propiedad intelectual o que en cumplimiento a funciones, facultades y atribuciones se haya generado en INDETEC, sin haber obtenido previamente la autorización correspondiente. Tampoco podrá distribuir información clasificada como reservada o confidencial.
13. El personal dará aviso a la Coordinación de cualquier evidencia o sospecha de mal uso del equipo de cómputo, internet y resguardo de la información.
14. El Personal no podrá otorgar acceso a personas ajenas a INDETEC a los servicios de red mediante su cuenta institucional. En situaciones extraordinarias en las que se requiera dar acceso a estas personas se deberán considerar los puntos siguientes:
    a) Supervisar y monitorear en todo momento el uso de los activos de TIC.
    b) En caso de requerir enviar información contenida en los activos de TIC será bajo el consentimiento expreso del personal que otorgó el acceso, quien se asegurará que no se vulneren los preceptos contenidos en el presente ordenamiento.
15. El personal es responsable de las transmisiones efectuadas por sus equipos en la red institucional y debe notificar qué puertos de comunicación son necesarios para llevar a cabo dichas actividades. Se debe tener en cuenta que eventos no previstos pueden ser bloqueados. Además, se realizarán auditorías periódicas para garantizar el

cumplimiento de la política de acceso y detectar posibles violaciones al firewall.

16. El Personal deberá bloquear los equipos a su resguardo en el momento en que no esté presente en su espacio de trabajo o cuando los equipos queden desatendidos. Esta medida tiene como finalidad prevenir el uso indebido de los equipos en ausencia del responsable, garantizando la seguridad y confidencialidad de la información almacenada en los mismos.
17. En situaciones en las cuales el personal cuente con un equipo institucional bajo su responsabilidad y deba realizar comisiones de trabajo fuera de las instalaciones de INDETEC, la salida de dichos activos TIC será posible únicamente con la previa autorización de su Jefe correspondiente. Este procedimiento garantiza un control adecuado y la supervisión necesaria para preservar la integridad de los activos y la seguridad de la información asociada.
18. El usuario del activo tecnológico que esté autorizado a realizar trabajo en modalidad remota deberá acudir periódicamente al centro de trabajo en los tiempos y plazos que establezca la Coordinación para la revisión del equipo y respaldo de la información contenida en este. En caso de ser necesario se habilitará el acceso a un espacio para que se realice el respaldo de manera periódica.
19. En el caso de que el personal sea víctima de robo, pérdida o extravío de equipo TIC institucional, se requerirá que notifiquen de inmediato a su jefe de área, además de a recursos materiales y soporte técnico interno. Estos les proporcionarán la información necesaria para presentar y ratificar la denuncia correspondiente ante las autoridades competentes. El propósito de esta acción es dejar constancia de los hechos, facilitar la activación de garantías y asegurar la adecuada actualización del inventario de activos, cumpliendo así con los procesos establecidos en el Instituto.
20. El personal será responsable de aplicar el antivirus instalado por la Coordinación antes de ejecutar cualquier dispositivo de almacenamiento externo (USB, Smartphone, disco duro externo, fuentes de información externas, etc.).
21. La Coordinación se reserva el derecho de acceder a páginas restringidas, otorgando dicho acceso exclusivamente mediante solicitud expresa del área interesada, preferiblemente a través de correo electrónico para registrar de manera efectiva dicha petición. Esta autorización estará sujeta a la existencia de un correo escrito, por el Titular de la Dirección de Área correspondiente al personal involucrado. El correo de autorización deberá detallar las actividades que el personal necesita llevar a cabo, ofreciendo la flexibilidad de establecer un periodo temporal o permanente según las necesidades específicas del área solicitante.
22. El servicio de internet suministrado, ya sea por cable o de manera inalámbrica, debe utilizarse exclusivamente para llevar a cabo actividades que respalden y mejoren las funciones específicas del trabajo asignado

por el Instituto. En relación con el intercambio de archivos, se insta a priorizar el uso de plataformas autorizadas por el Instituto, como lo son las carpetas en servidores o plataformas con licencia, entre las cuales se incluye WeTransfer. Se prohíbe estrictamente el acceso y uso de sitios de intercambio de archivos no autorizados.

23. El acceso a todas las páginas y sitios web a través del servicio de internet están sujetas a revisión por parte de la Coordinación.
24. Toda actividad realizada con el servicio de navegación en internet es única responsabilidad del usuario.
25. Se prohíbe el acceso a los sitios o páginas web que contengan materiales pornográficos, racistas, sexistas o cualquier otro tema que atente contra la dignidad humana. Para el caso de sitios de redes sociales, blogs, web de comentarios y páginas de intercambio de documentación que sean catalogados como amenazadores, el personal deberá solicitar la autorización para su acceso vía correo electrónico a la Coordinación, debiendo el usuario justificar debidamente por qué es necesario para el desarrollo de sus funciones institucionales.
26. El personal no deberá publicar o divulgar información confidencial relacionada con INDETEC a menos que dicha información deba volverse pública de acuerdo a las disposiciones del Instituto. La excepción sólo aplicará al personal que deba atender las funciones pertinentes o que cuente con autorización expresa por parte de la Coordinación.
27. El personal tiene la responsabilidad de notificar a la Coordinación sobre cualquier actividad sospechosa vinculada a la seguridad de la conectividad de internet, aplicaciones y correo electrónico, abarcando también casos de spam, así como posibles anomalías en los equipos de cómputo, etc.
28. El personal no utilizará los servicios de internet para fines ilegales. En caso de no estar seguro de la legalidad de sus acciones, deberá solicitar información a la Coordinación.

USO DE CONTRASEÑAS INSTITUCIONALES

1. Es responsabilidad del personal salvaguardar y gestionar con cautela los identificadores de usuario, claves de acceso, contraseñas, y demás datos asociados a los aplicativos informáticos proporcionados por INDETEC. Para asegurar la integridad de esta información, se aconseja no compartirla con terceros y evitar su almacenamiento en lugares visibles o accesibles a personas no autorizadas.
2. Se aconseja al personal restringir el número de intentos fallidos de acceso antes de bloquear la cuenta de forma temporal. Sin embargo, en el caso de que el personal bloquee accidentalmente algún aplicativo informático debido a intentos fallidos, se requiere notificar por escrito a la Coordinación y solicitar formalmente la reactivación correspondiente. Este procedimiento garantiza una gestión eficiente y una pronta resolución en caso de bloqueo involuntario.
3. Si el personal necesita generar una contraseña, se sugiere que su longitud sea mayor de 8 caracteres, incorporando en esta una mezcla de caracteres, como letras mayúsculas y minúsculas, números y caracteres especiales (@, #, $, etc.). Se recomienda evitar utilizar información personal o palabras comunes en la creación de contraseñas. Un ejemplo de contraseña segura podría ser: TruCo*78!aS.
   Recuerda que la seguridad de tus cuentas también depende de la protección de tus dispositivos y la conciencia sobre posibles amenazas.

USO DE UNIDADES EXTRAÍBLES

1. Al emplear medios removibles, tales como memorias USB, discos duros externos y tarjetas de memoria, se debe tener en cuenta que siempre existe un riesgo potencial para la seguridad. Es imperativo ser plenamente consciente de las amenazas asociadas con el uso de estos dispositivos y adoptar medidas eficaces para mitigar cualquier riesgo. En este contexto, el personal tiene la responsabilidad encarecida de escanear estos medios con un programa antivirus antes de su conexión para garantizar la detección temprana y la prevención de posibles amenazas.
2. Los medios removibles deben limitarse exclusivamente al transporte de información digital y no deben considerarse como un medio de respaldo debido a las siguientes desventajas:

    a. **Falta de privacidad de los datos:** En caso de olvido o pérdida cualquier persona podría acceder a la información, lo que implica un riesgo para la privacidad.

    b. **Vulnerabilidad a fallos:** Existen diversas razones por las cuales estos medios pueden dejar de funcionar, como variaciones de voltaje durante la conexión, su limitado tiempo de vida útil o daños por caídas al suelo, entre otros.

    c. **Facilidad de pérdida:** Debido a su tamaño, los medios removibles pueden extraviarse con facilidad o ser olvidados en algún dispositivo o espacio no óptimo, lo que aumenta el riesgo de pérdida de datos.

    d. **Susceptibilidad a virus:** Al poder ser utilizados en cualquier equipo de cómputo los medios removibles son propensos a ataques de virus, lo que compromete la integridad de los datos almacenados en ellos.

CORREO ELECTRÓNICO

1. El correo electrónico se presenta como una herramienta fundamental para la comunicación e intercambio oficial de información entre nuestro personal y las entidades públicas con las que mantenemos contacto. No obstante, es crucial señalar que su diseño no está orientado a la difusión masiva de información, como se requiere respecto a notificaciones de cursos, publicaciones, webinars, etc. Para llevar a cabo las tareas de notificación de manera efectiva, resulta imperativo emplear una herramienta adecuada e institucional que garantice un proceso de difusión eficiente y acorde con nuestros protocolos. Esto no solo optimizará el flujo de información, sino que también mitigará el riesgo de que nuestro correo no llegue correctamente a los entes con los cuales estamos en contacto. En este sentido, es recomendable priorizar el uso de la herramienta de envío masivo institucional, la cual permite gestionar

listas de distribución de manera eficiente. Esta herramienta posibilita la revisión constante de la actividad de los correos electrónicos, facilitando la identificación de aquellos que ya no están en uso. Esto, a su vez, permite una limpieza regular de las listas de correo de difusión, garantizando un proceso más efectivo y evitando el envío de información a direcciones obsoletas o no utilizadas.

2. La Coordinación será la instancia facultada para otorgar las cuentas de correo electrónico, de acuerdo a criterios internos y estructura organizacional.
3. La cuenta de correo asignada al personal deberá ser utilizada para actividades que estén relacionadas con los propósitos y funciones institucionales, agrupándose estos exclusivamente en contenidos académicos, administrativos y de investigación. Debido a esto, se considera el servicio de correo electrónico de INDETEC como una herramienta puesta al servicio del personal para el uso controlado y limitado a su trabajo, y no de uso personal pues solo debe emplearse información relacionada con las actividades propias del Instituto.
4. Los correos electrónicos asignados al personal del Instituto y la información contenida en ellos se consideran como propiedad del INDETEC.

ENVÍOS MASIVOS

Se considera un envío masivo aquel correo electrónico que tiene más de 20 destinatarios.

Solicitud de Correo Electrónico:

Los correos electrónicos pueden ser solicitados o no solicitados. Los correos solicitados son aquellos para los cuales los destinatarios han dado su consentimiento explícito para recibir comunicaciones de INDETEC. Los correos no solicitados son aquellos enviados a destinatarios que no han solicitado recibir información de INDETEC.

Tipos de Comunicados:

- Promocionales: Son aquellos correos electrónicos que promueven los servicios o productos de INDETEC, y no deben usar el dominio indetec.gob.mx. Para este propósito la Coordinación asignará dominios específicos.
- De servicio: Son aquellos correos electrónicos utilizados durante la prestación de servicios a nuestros clientes, estos envíos podrán usar el dominio indetec.gob.mx.

Directrices para envíos masivos:

- Consentimiento: Solo se enviarán correos electrónicos a destinatarios que hayan dado su consentimiento explícito para recibir comunicaciones de INDETEC, a menos que el correo sea de servicio y esté directamente relacionado con una transacción o servicio solicitado por el ente o funcionario.
- Relevancia: Los correos electrónicos deben ser relevantes para los destinatarios y estar alineados con sus intereses y preferencias.
- Transparencia: Todos los correos electrónicos deben incluir información clara sobre la identidad del remitente y ofrecer una forma fácil para que los destinatarios puedan optar por no recibir futuras comunicaciones.
- Cumplimiento legal: Todos los envíos masivos deben cumplir con las leyes y regulaciones locales y regionales relacionadas con la privacidad y el marketing por correo electrónico.
- Frecuencia: Limitar la frecuencia de los envíos masivos para evitar saturar a los destinatarios y garantizar que los correos electrónicos sean bien recibidos.

Responsabilidad de los empleados:

Es responsabilidad de los empleados que realicen envíos masivos garantizar la calidad del contenido del mensaje y asegurarse de que las listas de destinatarios estén actualizadas y contengan únicamente correos de personas que han autorizado recibir nuestras comunicaciones.

También es responsabilidad de los empleados atender los rebotes y responder de manera adecuada a cualquier consulta o comentario relacionado con los envíos.

ASIGNACIÓN DE NOMBRES DE USUARIOS

Los criterios y reglas generales para la asignación de nombre de usuario para el correo electrónico, nombre de equipo, acceso a aplicaciones, etc. se encuentran disponibles para consulta y observación de los responsables de las áreas técnicas, procurando la estandarización de estos datos dentro del Instituto.

La nomenclatura para generar el nombre de usuario estará basada en los siguientes criterios:

Primera letra del primer nombre + primer apellido + primera letra del segundo apellido

Ejemplo:

Nombre de la persona	Usuario
Juan Manuel López Jiménez	jlopezj

La Coordinación será la encargada de la definición de cuentas de usuario que serán asignadas a las áreas. En caso de existir construcciones similares o controversias se elaborarán procedimientos alternos para resolver dichas problemáticas, todo esto apegado al punto anterior.

TIPOS DE BUZONES

El perfil de usuario determinará las características con las que contará la cuenta o el buzón de correo electrónico de la siguiente manera:

1. El intercambio de correos, tanto en el envío como en la recepción, se verá restringido a un tamaño máximo de 20 MB. Esta limitación obedece a los estándares establecidos para el envío de correos electrónicos. En situaciones en las que sea necesario compartir archivos de mayor capacidad, se solicitará a los usuarios compartir un enlace que dirigirá al archivo correspondiente, permitiendo así la transferencia eficiente de información sin comprometer la integridad del sistema de correo electrónico.
2. La cantidad de destinatarios por correo electrónico se restringirá a un máximo de 20. Después de enviar un correo con estas características, será necesario esperar un periodo de treinta minutos antes de poder realizar otro envío similar. En caso de necesitar aumentar la cantidad de destinatarios permitidos, se requerirá contactar a la Coordinación para solicitar la autorización correspondiente. Esta medida busca gestionar de manera eficiente el flujo de correos electrónicos y garantizar un uso adecuado de los recursos del sistema.
3. Además de la posibilidad de consultar los correos electrónicos a través del aplicativo de Outlook previamente configurado por el área de soporte técnico en su equipo institucional, también se brinda la opción de acceder y revisar los correos electrónicos mediante la página http://webmail.indetec.gob.mx. Esto proporciona flexibilidad al personal, permitiéndoles acceder a su correo electrónico desde diferentes plataformas y dispositivos, de acuerdo con sus necesidades y preferencias.

CAPACIDAD DE ALMACENAMIENTO EN BUZONES

La capacidad del buzón de cada usuario está sujeta al almacenamiento del servidor de correo, y esta capacidad está directamente relacionada con las actividades realizadas a través del correo electrónico. Como norma general, se asigna inicialmente a cada usuario una capacidad de 250 MB, la cual se ajustará posteriormente de acuerdo con las necesidades específicas de las actividades institucionales. Estas medidas se implementan para asegurar el correcto funcionamiento del servicio de correo electrónico.

VIRUS Y CÓDIGO MALICIOSO

1. El personal no podrá descargar u obtener aplicativos de internet para la instalación en sus equipos de cómputo sin antes ser revisados y autorizados por la Coordinación.
2. El personal no descargará o en su defecto abrirá archivos adjuntos de correos electrónicos provenientes de fuentes desconocidas, sospechosas o poco confiables. Estos correos deberán ser notificados a la Coordinación para después ser eliminados inmediatamente del buzón.
3. Todos los archivos adjuntos sin excepción que se reciban vía correo electrónico serán revisados a través de los aplicativos que implemente la Coordinación antes de ser abiertos o almacenados en los equipos de cómputo de INDETEC. Esto con la finalidad de detectar la presencia de virus o alguna otra amenaza informática.
4. El personal no podrá realizar modificaciones en la configuración, así como desactivar el análisis en tiempo real del aplicativo de antivirus.
5. El personal utilizará únicamente el aplicativo antivirus proporcionado e instalado por la Coordinación y no podrá instalar o sustituir con algún otro aplicativo de antivirus.
6. El personal deberá de forma inmediata reportar a la Coordinación cualquier incidente de virus o código malicioso detectado por el aplicativo instalado.
7. El personal deberá, en la medida de lo posible, evitar compartir información de su equipo de cómputo con acceso de lectura y escritura, salvo en los casos que se cuente con autorización en cumplimiento de alguna disposición aplicable al INDETEC.

RESPALDOS

1. Las políticas institucionales de respaldo en INDETEC están diseñadas para garantizar la protección adecuada de los datos sensibles y críticos. Estas políticas se basan en la seguridad de la información y la continuidad del servicio para salvaguardar la integridad y confidencialidad de los datos.
2. El personal deberá identificar e informar a la Coordinación sobre cuál información contenida en los activos TIC sea fundamental, cuya destrucción, pérdida o alteración tendría grave impacto o consecuencia para el INDETEC.
3. El personal mantendrá organizada su información en expedientes electrónicos de fácil ubicación e identificación para efectos de respaldo y restauración de la misma.

4. Es responsabilidad del poseedor de la información asegurarse de contar con una copia de la misma, así como de proporcionar dicha información (versión final) a su supervisor inmediato. Del mismo modo, es responsabilidad del supervisor inmediato solicitar un espacio adecuado para almacenar esta información.
5. La Coordinación proporcionará los recursos necesarios para que tanto los poseedores de la información como los supervisores realicen respaldos periódicos según las necesidades de su unidad administrativa.
6. La Coordinación determinará el mecanismo de respaldo de la información en activos TIC en un lugar alterno al INDETEC para garantizar la continuidad en la operación y servicio.

MONITOREO DE USUARIOS

1. La Coordinación podrá realizar el monitoreo de correos electrónicos institucionales del personal, los directorios, archivos y otra información almacenada en los equipos de cómputo en cualquier momento y sin previo aviso. Asimismo, llevará el registro de incidencias y vulneraciones que pongan en riesgo la seguridad de la información de INDETEC, dando cumplimiento al marco legal y regulatorio vigente en la materia.
2. Los aplicativos informáticos de INDETEC y toda aquella información contenida en ellos son propiedad del Instituto y son auditables. La información contenida en los aplicativos anteriormente referidos pueden ser revisados, divulgados o interceptados por "El Instituto" en cualquier momento y sin previo aviso para vigilancia y control.

CONSIDERACIONES

Para los casos que no estén contemplados o considerados en las presentes POLÍTICAS DE USO DE EQUIPO DE CÓMPUTO, INTERNET Y RESGUARDO DE INFORMACION, será responsabilidad de la Coordinación el análisis y la resolución de los mismos, así como el realizar las adecuaciones pertinentes en las futuras versiones quedando plasmadas en la bitácora de control de cambios.
Será considerada como clasificada toda información relacionada con la asignación o uso de contraseñas; la contenida en los registros de incidencias y vulneraciones; y aquella derivada de la implementación de las presentes Políticas, en la que la Coordinación determine que su difusión constituya riesgo para la seguridad de la información en poder del Instituto, la protección de datos personales y activos TIC. De este modo, de ser necesario dicha Coordinación procederá al resguardo y salvaguarda de la información atendiendo los protocolos de seguridad y resguardo que la normatividad aplicable le determine al INDETEC.

ANEXO 1

Glosario de Términos:

POLITICAS DE USO DE EQUIPO DE CÓMPUTO, INTERNET Y RESGUARDO DE INFORMACION

- **Activo de información.** La información, los datos y los recursos que la contienen, procesan y transmiten, que, por su valor, deben ser cuidados y protegidos.
- **Amenaza.** Es el posible acto tanto interno como externo que puede afectar, a un activo de información
- **Arquitectura tecnológica.** Es la estructura de hardware, software y redes de telecomunicación requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC.
- **Autenticación electrónica.** Es el procedimiento informático que permite identificar de manera individual los atributos de un usuario, con la finalidad de que éste pueda acceder a un aplicativo o a un servicio electrónico.
- **Borrado seguro.** Se trata del proceso mediante el cual se elimina de manera permanente y no recuperable la información contenida en medios de almacenamiento digital.
- **Centro de Datos.** Es el espacio físico donde se concentran los recursos necesarios, consistentes en equipo informático y redes de

comunicaciones para el procesamiento de la información de una Institución.

- **Componente tecnológico.** Es el producto de hardware o software con una funcionalidad específica que permite proporcionar un beneficio integral o mayor funcionalidad técnica.
- **Coordinación.** Coordinación General de Administración y Finanzas
- **Datos abiertos.** Son los datos digitales de carácter público que pueden ser usados, reutilizados y redistribuidos por cualquier usuario.
- **Estrategias de Control.** Se refiere a las medidas establecidas para preservar la confidencialidad, integridad y disponibilidad de los activos de información contra las amenazas existentes y/o potenciales y que forman parte del proceso de administración de riesgos
- **Firma Electrónica Avanzada.** Se refiere al conjunto de datos y caracteres que permite la identificación del firmante, creada por medios electrónicos, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa.
- **Gobierno Digital.** Son las actividades basadas en tecnologías de información y comunicación que el Estado desarrolla para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los ciudadanos y dar transparencia a las acciones de gobierno.
- **Herramienta de envió masivo institucional.** PhpList es un software de código abierto para la gestión de listas de correo electrónico. Está diseñado para la divulgación de información -como boletines, novedades, publicidad- a una lista de suscriptores.
- **Incidente de seguridad.** Se refiere al evento o serie de eventos de seguridad de la información no deseados o inesperados, con impacto y probabilidad significativa de comprometer la continuidad de operaciones, las funciones esenciales de la Institución y amenazar la seguridad de la información.
- **Infraestructura de TIC.** ES el hardware, software, aplicativos de cómputo, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.
- **Interoperabilidad.** Es la capacidad de organizaciones y sistemas dispares y diversos, para interactuar con objetivos consensuados y comunes con la finalidad de obtener beneficios mutuos y donde se intercambia infraestructura de TIC.

- **Inventario de bienes y servicios de TIC.** Es el listado que comprende el equipo de cómputo (hardware), aplicaciones, software, bases de datos, servicios e infraestructura de la Institución.
- **Niveles de servicio.** Se refiere al establecimiento de las características y parámetros de un servicio contratado incluyendo la definición, disponibilidad, calidad, tiempos de respuesta y solución.
- **Plan de continuidad de operaciones.** Se refiere al instrumento Institucional que indica los insumos técnicos, humanos, funciones específicas y organización interna que garanticen la continuidad de las operaciones tecnológicas en las Instituciones.
- **Procesamiento de Datos.** Es el tratamiento de datos que se lleva a cabo de manera automática por medio de sistemas o aplicativos de cómputo.
- **Proceso esencial.** Es el que está relacionado con la generación y entrega de valor al entorno, ya sea en forma de productos o servicios; representa las actividades clave de la Institución para alcanzar sus objetivos.
- **Riesgo.** Se refiere a la probabilidad de que una amenaza pueda afectar una vulnerabilidad, generando un impacto o pérdida sobre la infraestructura de TIC y los activos de información de la Institución.
- **Seguridad de la Información.** Es la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad y trazabilidad.
- **Servicios en la Nube.** Es el modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente, que se encuentren localizados fuera o dentro del territorio nacional.
- **Software Libre.** Es el programa informático cuyo código fuente cumple con las cuatro Libertades del Software Libre y por ende se encuentra disponible para ser ejecutado, estudiado, modificado o distribuido libremente.
- **Tecnologías de la Información y Comunicación.** Se refiere al equipo de cómputo, software, dispositivos de impresión, infraestructura y servicios que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.
- **Trabajo Presencial.** El trabajo presencial implica desempeñar funciones laborales en una ubicación física designada por la empresa.

- **Trabajo Remoto.** El trabajo remoto, también conocido como teletrabajo o *home office*, implica realizar las tareas laborales desde cualquier ubicación fuera de la oficina tradicional acordado por la empresa.
- **Vulnerabilidad.** a la debilidad presente en un activo de información que potencialmente permitirá que una amenaza lo impacte de manera negativa, con posibles afectaciones para la seguridad de la información dentro de la Institución.

BITÁCORA DE CONTROL DE CAMBIOS

Descripción del cambio	Impacto	Fecha de evaluación	Aprobador	Aceptado/Rechazado	Fecha de aplicación
N/A	N/A	N/A	N/A	N/A	N/A

HOJA DE IDENTIFICACIÓN DE FIRMAS

Versión: v1.1
Fecha: 12/06/2024

Descripción:
POLÍTICAS DE USO DE EQUIPO DE CÓMPUTO, INTERNET Y RESGUARDO DE INFORMACIÓN

Políticas	*Fundamento*		*Aplicación*
POLÍTICAS O TIC-INDETEC	MAAGTIC-SI		10/07/2024
Elaboró	*Fecha* 12/06/2024	***Autorizó***	*Fecha* 09/07/2024

INTEGRANTES DEL COMITÉ DE SEGURIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓNES (CSTIC)

Mtro. Carlos García Lepe
Director General de INDETEC y Presidente del CSTIC

Mtro. Mario Rodríguez Somohano
Subcoordinador en Tecnologías de la Información y Comunicaciones y Coordinador del CSTIC

Dr. Ramón Castañeda Ortega
Director Especial de Atención a los Organismos del Sistema Nacional de Coordinación Fiscal, Vocal del CSTIC

Mtro. José Luis Flores Mota
Director Especial de Hacienda Municipal y Vocal del CSTIC

Mtro. Gustavo Adolfo Aguilar Espinosa de los Monteros
Coordinador General de Administración y Finanzas y Vocal del CSTIC

Mtra. Laura Mejía Vázquez
Subcoordinadora en SAACG.NET y Vocal del CSTIC

Ing. Israel Medrano Bocanegra
Subcoordinador en Desarrollo de Sistemas y Vocal del CSTIC

Mtro. Bernardo Cabrera González
Especialista en Administración de Riesgos y Vocal del CSTIC

Ing. Emmanuel Hernández González
Soporte Tecnológico Interno y Vocal del CSTIC

T.P.I Ramiro de Jesús Ambario Lomelí
Técnico en Informática (Soporte Tecnológico Interno) y Vocal del CSTIC

Jairo A. Navarro S.

Ing. Jairo Alejandro Navarro Serrano
Administrador de Infraestructura y Vocal del CSTIC

Ing. Mónica Ramos Marín
Desarrolladora Web y Secretaria Técnica del CSTIC