ACUERDO DEL DIRECTOR GENERAL DEL SISTEMA ESTATAL DE TELECOMUNICACIONES MEDIANTE EL CUAL SE ESTABLECEN LOS CONTROLES DE SEGURIDAD TECNOLOGICA DEL ORGANISMO PUBLICO DESCENTRALIZADO "SISTEMA ESTATAL DE TELECOMUNICACIONES".

Para los efectos del presente acuerdo se entenderán por:

ABD: Administrador de Base de Datos.
AREA DE TELECOMUNICACIONES: Oficina que cuente con equipamiento de cómputo, transmisores o enlaces de telecomunicación.
ASC: Área de Seguridad en Cómputo (Áreas de seguridad en: Informática y TICS). Se encarga de definir esquemas y políticas de seguridad en materia de cómputo para la entidad.
ATI: Administrador de Tecnologías de Información (Tecnologías Digitales). Responsable de la administración de los equipos de cómputo, sistemas de información y redes de telecomunicaciones de la Entidad.
BASE DE DATOS: Almacén que permite guardar grandes cantidades de información de forma organizada en el sistema de respaldo LTO8 y/o sistema de Almacenamiento de Red (NAS).
CAV: Central Antivirus.
CENTRO DE OPERACIONES DE LA RED: Es el área que se encarga del funcionamiento y operación de las Tecnologías de Información y comunicaciones en el Sistema Estatal de Telecomunicaciones.
CONTRASEÑA: Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).
CORREO ELECTRONICO: Servicio de Red que permite a los usuarios enviar y recibir mensajes rápidamente mediante sistemas de comunicación electrónicos.
EQUIPO: Entiéndase por dispositivo de audio, video, videograbadora, reproducción, consolas de audio y de video, computo, impresoras y telecomunicaciones
INTERNET: Conjunto descentralizado de redes de comunicaciones interconectadas, que utilizan la familia de protocolos TCP/IP de alcance mundial.
RECURSO INFORMÁTICO: Cualquier componente físico o lógico de un sistema de información.
RED: Conjunto de equipos de cómputo interconectados, a sistemas de información y telecomunicaciones.
SITE: Espacio designado en la entidad a los equipos de telecomunicaciones y servidores.

SOLUCIÓN ANTIVIRUS: Recurso informático empleado en la red para solucionar problemas causados por virus informáticos.
TELEMÁTICA: Conjunto de servicios y técnicas que asocian las telecomunicaciones y la informática ofreciendo posibilidades de comunicación e información.
TIC: (Tecnologías de Información y Comunicaciones) conjunto de teorías y de técnicas que permiten el aprovechamiento práctico de la Información.
USUARIO: Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por el Sistema Estatal de Telecomunicaciones tales como equipos de cómputo, sistemas de información, redes de información, etc.
VIRUS INFORMÁTICO: Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

CAPÍTULO 1
DISPOSICIONES GENERALES

ARTÍCULO 1º ÁMBITO DE APLICACIÓN Y FINES.

1.1 Los Controles de Seguridad Tecnológica del Organismo Público Descentralizado “Sistema Estatal De Telecomunicaciones” tienen por objeto promover, consolidar y hacer del conocimiento de los servidores públicos las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información, sistemas de comunicación y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de equipos del Organismo.

1.2 El Organismo a través de la Dirección General dará a conocer estos controles de seguridad debidamente asistido por la Subdirección de Tecnologías Digitales.

1.3 La Dirección General aprobará las guías de uso y políticas particulares complementarias al presente instrumento de acuerdo a su naturaleza y necesidades.

1.4 La Subdirección de Tecnologías Digitales será la responsable de hacer cumplir estos controles, así como los establecidos en las demás

normatividad aplicable al respecto, coordinándose para tal efecto con las demás unidades administrativas del Organismo.

1.5 La Subdirección de Tecnologías Digitales deberá informar de manera inmediata a la Dirección General sobre los incumplimientos o violaciones detectados al respecto de los presentes controles de seguridad.

ARTÍCULO 2º EVALUACIÓN DE LOS CONTROLES DE SEGURIDAD TECNOLÓGICA.

2.1 La Subdirección de Tecnologías Digitales evaluará dicho instrumento con una frecuencia semestral, presentando propuestas de modificaciones, en caso de existir.

2.2 La Dirección General evaluará el contenido del presente instrumento en cualquier momento, a efecto de poder realizar las modificaciones que considere pertinentes.

CAPÍTULO 2
CONTROL DE SEGURIDAD FÍSICA

ARTÍCULO 3º ACCESO FÍSICO

3.1 Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada, de manera que el usuario no tenga acceso físico directo.

3.2 El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso al edificio.

3.3 Las visitas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas por personal responsable del área y con el permiso por medio escrito o electrónico del director de área correspondiente en horarios previamente establecidos.

3.4 El personal de la Subdirección de tecnologías Digitales es el único facultado para mover, cambiar o extraer equipo de cómputo de las unidades administrativas del Organismo dentro de las instalaciones del mismo, previo acuerdo con el Director del Área, el cual notificará al Departamento de Recursos Materiales para los efectos administrativos correspondientes.

3.5 Para extraer equipo de las instalaciones del Organismo se requiere autorización de las Subdirecciones de Recursos Materiales y Tecnologías Digitales, notificando al personal de seguridad para los efectos administrativos correspondientes.

ARTÍCULO 4º RESGUARDO DE LOS EQUIPO

4.1 La Subdirección de Recursos Materiales será la que determine los procedimientos para inventario físico, firmas de resguardo, préstamos y usos de equipos tecnológicos.

4.2 El resguardo de los equipos deberá quedar asignado a la persona que los usa o administra, permitiendo conocer siempre la ubicación física de los equipos.

4.3 El centro de operaciones, así como las áreas que cuenten con equipos de misión crítica deberán contar con vigilancia y/o algún tipo de sistema que ayude a recabar evidencia de accesos físicos a las instalaciones.

ARTÍCULO 5º PROTECCIÓN FÍSICA

5.1 El acceso al SITE será controlado por la Subdirección de Tecnologías Digitales, a través de los medios que para tal efecto establezca.

5.2 LAS ÁREAS DE TELECOMUNICACIONES deberán:

a) Recibir obligatoriamente limpieza al menos una vez por semana.
b) Ser un área restringida.
c) Tener instalaciones eléctricas en buen estado.
d) Contar por lo menos con dos extintores especializados para equipo electrónico, mismo que deberán ser revisados semestralmente.

5.3 LAS ÁREAS DE TELECOMUNICACIONES deberán seguir los estándares aplicables vigentes para una protección adecuada de los equipos y servidores.

5.4 Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas de LAS ÁREAS DE TELECOMUNICACIONES deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

5.5 Cada vez que se requiera conectar equipos, se deberá comprobar la carga de las tomas de corriente.

5.6 Las áreas de ingenierías deberán contar con un Plan de Recuperación de Desastres que asegure la continuidad del servicio.

ARTÍCULO 6º RESPALDOS

6.1 La Base de Dato del Organismo será respaldada periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.

6.2 Los respaldos del Organismo deberán ser almacenados en un Centro de Datos que cuente con todas las especificaciones internacionales de seguridad.

CAPÍTULO 3
POLÍTICAS DE SEGURIDAD LÓGICAS DE LOS SISTEMAS DE TELECOMUNICACIONES DEL ORGANISMO

ARTÍCULO 7º DE LA RED

7.1 Los Sistemas de Telecomunicaciones del Organismo tienen como propósito principal servir en la transportación e intercambio de información entre usuarios, así como con la Red Estatal de Educación, Salud, Gobierno, otras dependencias y entidades estatales, nacionales e internacionales.

7.2 La responsabilidad del contenido de datos por el tráfico que circula en la red recae en el usuario que genere y solicite la información.

7.3 Es obligación del resguardante del equipo respaldar la información almacenada en los equipos que se le hayan asignado para el desarrollo de sus funciones, debiendo entregar a la unidad administrativa correspondiente los respaldos de información institucional que obran en su poder al concluir una relación laboral o cambiar de adscripción.

7.4 La información almacenada en los equipos es propiedad del Organismo, por lo tanto, el servidor púbico resguardante del mismo no debe sustraerla, o realizar copias para fines distintos al institucional, absteniéndose de borrar o eliminar dicha información.

7.5 La Subdirección de Tecnologías Digitales generará al servidor público que tenga asignado un equipo una contraseña para uso personal absteniéndose de compartirla o divulgarla.

7.6 En el caso de utilizar equipo personal para el desarrollo de sus actividades la información deberá ser guardada en los sistemas de almacenamiento del Organismo, toda vez que dicha información es propiedad del mismo.

7.7 Las cuentas de ingreso a los equipos propiedad del Organismo se usarán exclusivamente para actividades relacionadas con la dependencia, mismas que son de carácter personal e intransferible.

7.8 En caso de olvido de contraseña, el usuario deberá solicitar de manera escrita la reasignación de contraseña a la Subdirección de Tecnología, previa autorización del titular de la unidad administrativa de su adscripción.

7.9 La Subdirección de Tecnologías Digitales se reserva el derecho de cancelar o inhabilitar cualquier cuenta o software cuyo usuario incurra en algún incumplimiento a todo lo anterior o que afecte la operación general del servicio.

7.10 Los sistemas de protección contra software malicioso deberán ser implementados en todos los equipos del Organismo.

7.11 Periódicamente se hará el rastreo en los equipos de cómputo del Organismo y se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

7.12 Los usuarios deberán evitar ingerir alimentos o bebidas en las áreas donde se encuentren instalados los equipos, siendo responsables del daño que se llegare a causar a los mismos por imprudencia, descuido, negligencia o mal uso en que llegare a incurrir.

ARTÍCULO 8º DEL ÁREA DE INGENIERÍA

8.1 La Subdirección de Tecnologías Digitales será la responsable de llevar un control total y sistematizado de los equipos de acuerdo al procedimiento que establezca para tal efecto.

8.2 La Jefatura de Soporte Técnico es la responsable de calendarizar y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos.

8.3 La Dirección Administrativa deberá reportar a la Subdirección de Tecnologías Digitales cuando un usuario deje de laborar o de tener una relación con el Organismo para los efectos de la cancelación o bajas de las cuentas institucionales bajo su resguardo.

8.4 Los administradores no podrán remover del sistema ninguna información de cuentas individuales, salvo que la información sea contraria a la ley, ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

ARTÍCULO 9º POLÍTICAS DE USO ACEPTABLE DE LOS USUARIOS Y MANEJO DE INFORMACIÓN

9.1 Los equipos utilizados por el usuario deberán:

a) Ser acordes al trabajo desarrollado.
b) Ser utilizados única y exclusivamente por personal del Organismo
c) Ser utilizados solo para fines institucionales.

9.2 Todos los usuarios deben respetar la confidencialidad de la información que se genere en cada uno de sus departamentos.

9.3 Es responsabilidad del servidor público el buen uso de la cuenta de correo electrónico asignada. Se entenderá por buen uso de correo electrónico lo siguiente:

9.3.1 transmitir y recibir información exclusivamente para propósitos institucionales y acorde a las funciones del puesto desempeñado.

9.3.2 evitar acciones que pongan en riesgo o degraden los servicios que se prestan a través de la red del Organismo o que afecten la integridad de los bienes informáticos.

9.4 La Subdirección de Tecnologías Digitales se reserva el derecho de cancelar o inhabilitar cualquier cuenta de correo electrónico institucional cuyo usuario incurra en algún incumplimiento al presente acuerdo o que afecte la operación general del servicio

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

9.6 Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los equipos del Organismo, de acuerdo con los controles de seguridad que en este documento se mencionan.

9.7 Los usuarios deberán solicitar apoyo al ATI ante cualquier duda en el manejo de los equipos del Organismo.

CAPÍTULO 4
POLÍTICAS DE SEGURIDAD LÓGICA PARA ADMINISTRACIÓN DE LOS RECURSOS DE CÓMPUTO

ARTÍCULO 10º ÁREA DE SEGURIDAD EN CÓMPUTO

10.1 La Subdirección de Tecnologías Digitales es la encargada de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo.

10.2 La Subdirección de Tecnologías Digitales pondrá a disposición de los usuarios el software que refuerce la seguridad de los sistemas de cómputo.

10.3 La Subdirección de Tecnologías Digitales deberá llevar a cabo campañas de difusión y capacitación en materia de prevención de ataques cibernéticos.

10.4 La Subdirección de Tecnologías Digitales es el único autorizado para monitorear constantemente el tráfico de información sobre la red, con el fin de detectar, solucionar anomalías y registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la Red.

ARTÍCULO 11º RENOVACIÓN DE EQUIPO

11.1 La renovación de los equipos se llevará a cabo tomando en consideración lo previsto en el Titulo Segundo Capitulo Único del ACUERDO del Secretario de Finanzas y Administración, por el cual establece la Normatividad en Materia de Tecnologías de la Información y Comunicación para las Dependencias y Entidades de la Administración Pública del Estado.

Artículo 12º SANCIONES

12.1 Cualquier conducta contraria a **LOS CONTROLES DE SEGURIDAD TECNOLOGICA DEL ORGANISMO PUBLICO DESCENTRALIZADO "SISTEMA ESTATAL DE TELECOMUNICACIONES",** será sancionada en los términos citados en el presente y en la normatividad aplicable al respecto.

ARTÍCULO 13º VIGENCIA

13.1 El presente acuerdo entrará en vigor a partir del 01 de agosto del 2021.

13.2. Se derogan todas aquellas disposiciones que sean contrarias al presente Acuerdo de Control de Seguridad.

13.3. Se ordena realizar su publicación en la página oficial del Organismo.

13.4. Se instruye hacer del conocimiento a todos los titulares de las Unidades Administrativas del Organismo para su difusión entre el personal a su cargo y a la Subdirección de Tecnologías Digitales para llevar a cabo la difusión y capacitación de **LOS CONTROLES DE SEGURIDAD TECNOLOGICA DEL ORGANISMO PUBLICO DESCENTRALIZADO "SISTEMA ESTATAL DE TELECOMUNICACIONES".**

SAN ANDRES CHOLULA, PUEBLA A 30 DE JULIO DEL 2021.

C. FERNANDO LUIS SANCHEZ MEJORADA Y ROJAS.

DIRECTOR GENERAL DEL ORGANISMO PUBLICO DESCENTRALIZADO "SISTEMA ESTATAL DE TELECOMUNICACIONES"

Sistema
Estatal de
Telecomunicaciones
Gobierno de Puebla

Blvd. Atlixcáyotl 1910,
Col. Reserva Territorial Atlixcáyotl,
San Andrés Cholula, Puebla, C.P. 72810

(222) 273 77 00

www.puebla.mx