POLÍTICAS PARA LA SEGURIDAD INFORMÁTICA.

I.- Introducción.-

La Seguridad Informática es un tema de especial relevancia para cualquier persona que tenga contacto con las Tecnologías de Información y Comunicaciones. Una administración eficiente de los recursos informáticos ayuda a mejorar la Seguridad Informática y la confianza del usuario en los sistemas informáticos sólo se puede lograr a través de una protección efectiva de los diferentes elementos que se integran en las plataformas de cómputo y comunicaciones que sirven para administrar, procesar e intercambiar la información.

Estos ambientes informáticos han sido sometidos a una constante evolución que permanentemente modifica las condiciones de trabajo de los sistemas y genera la aparición de nuevos riesgos y amenazas que deben atenderse para minimizar los efectos potenciales que puedan tener sobre la organización. Esta necesidad ha motivado el desarrollo del presente documento de políticas para la Seguridad Informática que se orientan principalmente al uso adecuado de las destrezas tecnológicas, hacer recomendaciones para obtener el mayor provecho de la tecnología y evitar su uso indebido, ya que esto puede ocasionar serios problemas a los bienes, servicios y operaciones del Ente público.

Por ello las presentes Políticas para la Seguridad Informática se plantean como una herramienta organizacional para alinear esfuerzos y crear conciencia entre los colaboradores y usuarios del ente público, sobre la importancia de mantener protegidos la información y los servicios tecnológicos que soportan las funciones del mismo ente. En este documento se propone una política de Seguridad Informática que requiere un alto compromiso con la dependencia, agudeza técnica para establecer fortalezas y detectar debilidades en su aplicación, y constancia para mantenerla actualizada de forma continua en función de los cambios tecnológicos que la influyen.

II.- Glosario.-

Para efectos de las presentes Políticas se entenderá por:

I. **Activos Informáticos:** Comprenden a los recursos informáticos tales como equipos de cómputo, los equipos de comunicaciones, el software, las bases de datos y archivos electrónicos que deben ser protegidos por el ambiente de Seguridad Informática del Ente público;

II. **Ambiente de Seguridad Informática:** Medidas de Seguridad Informática que se establecen en el ente público, con la finalidad de proteger sus activos informáticos, crear conciencia de la seguridad, incrementar el compromiso de su personal y garantizar la continuidad de las actividades del Ente público;

III. **Ambiente de Desarrollo:** Área donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas;

IV. **Ambiente de Producción:** Área donde se ejecutan los sistemas y se encuentran los datos de producción;

V. **Áreas de Acceso Restringido:** Comprenden las áreas de centro de cómputo, de pruebas, de procesamiento de Información, de suministro de energía eléctrica, de aire acondicionado, cuarto de máquinas, racks de comunicaciones, y cualquier otra área considerada crítica para el correcto funcionamiento de los Sistemas Electrónicos;

VI. **Autenticación**: Nivel de confianza recíproca suficiente sobre la identidad del Usuario y el Ente público;

VII. **Autorización:** Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. forma de comunicarlo al otro participante de la transacción electrónica;

VIII. **Confidencialidad**: Principio de la seguridad de la información que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma;

IX. **Control de Acceso:** Orientado a controlar el acceso lógico a la Información Electrónica;

X. **Desarrollo y Mantenimiento de los Sistemas:** Orientado a garantizar la incorporación de medidas de seguridad en los Sistemas de Información desde su desarrollo hasta su implementación y mantenimiento;

XI. **Disponibilidad**: Principio de la seguridad de la información que garantiza que los Usuarios autorizados tengan acceso a la información o a los recursos relacionados con la misma, toda vez que lo requieran;

XII. **Evaluación de Riesgos**: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las Instalaciones de Procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación del Ente público;

XIII. **Enlace Informático**: el servidor público designado por el Titular de cada Unidad Administrativa, como responsable para apoyar coordinación de la función informática al interior de la Unidad Administrativa de su adscripción;

XIV. **Integridad**: Principio de la seguridad de la información que garantiza y salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento;

XV. **Información electrónica institucional**: la información en formato electrónico o asimilable

directamente a través de un recurso informático que por su contenido resulte sensible, necesaria o valiosa para el desempeño de las funciones y obligaciones del ente público;

XVI. **Información electrónica sensible**: la información en formato electrónico o asimilable directamente a través de un recurso informático que sea valiosa para el Ente público y que deba ser protegida por ser confidencial y/o necesaria para la continuidad operativa o la realización de las funciones de una o varias áreas del ente público, la consecución de sus objetivos, o el cumplimiento de la normatividad vigente;

XVII. **Ente público**: Secretaría de Cultura del Estado de Colima;

XVIII. **No repudio**: se refiere a evitar que una persona que haya enviado o recibido información alegue ante terceros que no la envió o recibió;

XIX. **Soporte Móvil de Almacenamiento Informático removible**: Comprenden a los discos externos, USB, DVD´s, CD´s, cintas magnéticas, etc.;

XX. **Recurso Informático**: la persona, bien (tangible o intangible) o servicio que sea necesario para apoyar tareas relacionadas con la captación, el almacenamiento, el procesamiento, el acceso o la transmisión de información y/o datos utilizando medios electrónicos, ópticos o magnéticos;

XXI. **Planes de continuidad:** es la planificación que identifica el Ente público ante la exposición de amenazas internas y externas que ofrecen una prevención de recuperación de las operaciones del ente público, manteniendo la integridad del sistema;

XXII. **Plataforma de Seguridad Informática:** Conjunto de metodologías y herramientas informáticas que permiten proteger los sistemas y servicios informáticos del ente público, detectar amenazas informáticas y garantizar la continuidad de las actividades del Ente público;

XXIII. **Políticas:** Políticas para la Seguridad Informática del ente público;

XXIV. **Responsable de Desarrollo de Sistemas:** Es el encargado de la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas sus etapas;

XXV. **Responsable de Seguridad Informática:** Servidor público designado por el ente público como encargado de supervisar el cumplimiento de las presentes Políticas y de asesorar en materia de Seguridad Informática a los integrantes del Ente público que así lo requieran;

XXVI. **Responsable de Servicio Informático o Responsable de Servicio**: el servidor público designado por el ente público, que tenga a su cargo la responsabilidad sobre la coordinación y/o administración de un servicio informático;

XXVII. **Servicio Informático**: conjunto de las funcionalidades, reglas y recursos informáticos que sirven para satisfacer las necesidades del Ente público en un aspecto específico del campo de la informática o de las comunicaciones;

XXVIII. **Usuario de Sistemas y Servicios Informáticos:** Al personal del Ente público que haga uso de bienes, servicios, recursos informáticos o de información electrónica que sea responsabilidad del ente público; y

XXIX. **Usuario Externo:** A la persona externa (consultores, soporte de hardware, software, servicio social, estadías, prácticas profesionales, etc.) al Ente público que haga uso de bienes, servicios, recursos informáticos o de información electrónica que sea responsabilidad del ente público.

III-. Objeto.

Establecer la política institucional en materia de Seguridad Informática que apoye la Seguridad de la Información, entendida como la preservación de su integridad, confidencialidad y disponibilidad, así como instrumentar y coordinar acciones para minimizar daños a la infraestructura tecnológica y a los sistemas informáticos.

IV.- Marco Jurídico.

a) Constitución Política de los Estados Unidos Mexicanos.

b) Leyes.

b.1. Ley General de Archivos;

b.2. Ley Federal del Derecho de Autor;

b.3. Ley General de Transparencia y Acceso a la Información Pública,

b.4. Ley General de Responsabilidades Administrativas,

b.5. Código Penal Federal y

b.6. Ley de Archivos del Estado de Colima

b.7. Ley de Transparencia y Acceso a la Información Pública del Estado de Colima,

b.8. Ley de Fiscalización Superior y Rendición de cuentas del Estado de Colima.

c) Reglamentos.

c.1. Reglamento Interior de la Secretaría de Cultura y demás reglamentos del Ente público.

d) Lineamientos

d.1. Lineamientos del Portal Web Institucional, sus redes sociales, sitios y páginas;
d.2. Lineamientos generales para la administración y uso de las tecnologías de la información y comunicaciones en el ente público.

V.- Políticas Generales.

A.- Organización de la Seguridad Informática.

1.- El objetivo principal de la Seguridad Informática será proteger desde el ámbito tecnológico la información electrónica institucional, los recursos informáticos y los servicios tecnológicos necesarios para que el ente público pueda cumplir con las funciones y obligaciones que le correspondan de acuerdo a la normatividad aplicable.

2.- La Seguridad Informática en el ente público implica una responsabilidad a cargo de los administradores y usuarios de Sistema y Servicios Informáticos Institucionales.

3.- El Titular del ente público designará a un Coordinador y a un Responsable de la Seguridad Informática del ente público quienes le apoyarán con las labores relacionadas con la Seguridad Informática del mismo.

4.- El Coordinador de Seguridad Informática del ente público, tendrá las siguientes responsabilidades:

a) Proponer e integrar estrategias y elementos para conformar el Programa Institucional de Seguridad Informática alineados al Sistema de Seguridad de la Información, en coordinación con el Titular del ente público, los Enlaces Informáticos;

b) Coordinar los procesos y proyectos en materia de Seguridad Informática con los Enlaces Informáticos y con el Responsable de Seguridad Informática del ente público;

c) Mantener la coordinación en materia de Seguridad Informática con el área encargada del Sistema de Seguridad de la Información y con el área administrativa encargada de acceso a los edificios del ente público;

d) Establecer acuerdos en materia de Seguridad Informática con áreas internas e instituciones externas al ente público;

e) Proponer recomendaciones y acciones de aplicación general en materia de Seguridad Informática;

f) Proponer criterios en materia de Seguridad Informática para la clasificación, registro y protección de los recursos informáticos del ente público;

g) Publicar en la Intranet Institucional los documentos normativos en materia de Seguridad Informática emitidos; y

h) Las demás que determine el Titular del ente público;

5.- El Responsable de la Seguridad Informática del ente público, será el encargado de:

a) Coordinar con los Enlaces Informáticos y los responsables de servicio las acciones en materia de Seguridad Informática que deberán llevarse a cabo en el ente público;

b) Proponer políticas y especificaciones técnicas de bienes y servicios, procedimientos, acciones y medidas específicas en materia de Seguridad Informática; que sean aplicables a

cualquiera de los elementos tecnológicos que integren la plataforma de Seguridad Informática;

c) Mantener la administración del sistema de autentificación de usuarios que permite el acceso a los recursos y servicios informáticos y de comunicaciones del ente público;

d) Coordinar la definición, la administración y las acciones técnicas en materia de Seguridad Informática con los enlaces informáticos, los responsables de servicios, los administradores de servicios y con otras áreas que realicen funciones informáticas para el Ente público;

e) Del sistema de gestión de incidentes de seguridad de la información, analizar aquellos que involucren los servicios informáticos a fin de establecer controles para detectar, corregir y prevenir incidentes posteriores.

f) Proponer medidas específicas en materia de Seguridad Informática que deberán atender los usuarios de los bienes, de los recursos y servicios informáticos y de la información electrónica;

g) Proponer la plataforma tecnológica para el soporte del ambiente de Seguridad Informática del ente público;

h) Mantener actualizado el inventario de Activos Informáticos relacionados con la Plataforma de Seguridad Informática del ente público como complemento del inventario de activos de Información;

i) Realizar revisiones selectivas a los controles de los activos informáticos para asegurar que se mantenga sobre ellos la aplicación de las recomendaciones y lineamientos en materia de Seguridad Informática;

j) Establecer en coordinación con los Enlaces Informáticos y los responsables de servicio las ubicaciones y condiciones con que deberá realizarse el respaldo de la información electrónica;

k) Publicar en la Intranet Institucional los documentos técnicos en materia de Seguridad Informática emitidos;

l) Promover el cumplimiento de la normatividad informática en el ente público;

m) Definir controles de detección y prevención para la protección contra software malicioso;

n) Implementar controles para la protección contra software malicioso en la infraestructura de cómputo y telecomunicaciones;

o) Definir las cuentas de acceso para la administración de los equipos de cómputo para proteger la configuración de los mismos, las cuales hará del conocimiento a los Enlaces Informáticos;

p) Revisar los registros de eventos de los diferentes equipos que formen parte del ambiente de seguridad del ente público a fin de colaborar con el responsable del servicio en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad;

q) Almacenar y administrar las claves criptográficas incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados;

r) Revocar las claves criptográficas, cuando las claves estén comprometidas o cuando un

usuario que haga uso de ellas se desvincule del Ente público;

s) Recuperar las claves perdidas o alteradas como parte de la administración para su continuidad;

t) Coordinar, administrar y registrar todos los nombres de equipos y dominios que son accesibles en la Intranet y en Internet del ente público;

u) Controlar y registrar todos los certificados de seguridad de los sitios del ENTE PÚBLICO;

v) Coordinar los grupos de reacción inmediata y otros grupos de trabajo para manejar los reportes de incidentes y anomalías de Seguridad Informática;

w) Promover la cultura de la Seguridad Informática entre los administradores y usuarios de la información electrónica y de los recursos, bienes y servicios informáticos institucionales; y

x) Las demás que determine el Titular ente público o el Coordinador de Seguridad Informática.

6.- Los Enlaces Informáticos tendrán las siguientes responsabilidades con respecto a la Seguridad Informática en el Ente público:

a) Atender las disposiciones en materia de Seguridad Informática que se emitan en el ente público y promover el cumplimiento al interior de su Unidad Administrativa;

b) Establecer acciones al interior de su Unidad Administrativa para apoyar al cumplimiento del Programa Institucional de Seguridad Informática;

c) En coordinación con el Responsable de Seguridad Informática y los responsables de servicios, realizar ejercicios de análisis de riesgos que contribuyan a la continuidad operativa de los Servicios Informáticos y de Seguridad de la Información;

d) Coordinar al interior de su área las acciones para apoyar la ejecución de los Planes de Continuidad;

e) Verificar que se cumplan las condiciones establecidas por el ente público para proteger los Activos Informáticos relacionados con la Plataforma de Seguridad Informática del ente público que se encuentren asignados a su Unidad Administrativa;

f) Proporcionar información sobre los registros de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática del ente público que se encuentren asignados a su Unidad Administrativa;

g) Atender en coordinación con el responsable de Seguridad Informática cualquier hecho que ponga en riesgo el Ambiente de Seguridad Informática en su Unidad Administrativa;

h) Verificar las condiciones del Ambiente de Seguridad Informática de su Unidad Administrativa y proponer medidas para mejorarlo;

i) Verificar que todo equipo o medios de almacenamiento sujeto a reutilización que contenga información sensible sean borrados de forma permanente antes de su reasignación; y

B. - Administración de los Activos Informáticos.

1.- El Responsable de la Seguridad Informática emitirá el listado de Activos Informáticos relacionados con la Plataforma de Seguridad Informática.

2.- El Responsable de la Seguridad Informática deberá diseñar, implementar y mantener un inventario actualizado de los Activos Informáticos relacionados con la Seguridad Informática del ente público conforme al listado de Activos Informáticos.

3.- El Responsable de la Seguridad Informática propondrá un responsable para cada uno de los Activos Informáticos relacionados con el inventario mencionado en el numeral anterior.

4.- El Responsable de la Seguridad designará a cada uno de los responsables de los Activos Informáticos relacionados con la Seguridad Informática del ente público.

5.- Los responsables de los Activos Informáticos relacionados con la Seguridad Informática del ente público, deberán atender las siguientes funciones relacionadas con el activo del que sean responsables:

a) Mantener la información actualizada del activo en el registro correspondiente al activo informático del que sean responsables;

b) Establecer esquemas de protección del activo acordes a las recomendaciones, políticas y lineamientos que sean emitidos por el responsable de Seguridad Informática;

c) Atender a las medidas y disposiciones que emita el Responsable de la Seguridad Informática;

d) Atender a las medidas y disposiciones acordadas con el Responsable de la Seguridad Informática;

C.- Responsabilidades en Materia de Seguridad Informática para el Uso de Bienes, Servicios, Recursos Informáticos y de Información Electrónica.

1.- Todo Usuario de Recursos Informáticos tendrá las siguientes responsabilidades:

a) Atender las medidas de Seguridad Informática emitidas por el ente público que se encuentren publicadas en la Intranet Institucional;

b) Mantener bajo reserva las claves de usuario y los correspondientes códigos de acceso que le hayan sido asignadas por el ente público;

c) Bloquear el acceso a su equipo de cómputo cuando deba dejarlo desatendido por algún tiempo;

d) Almacenar bajo llave las computadoras portátiles y Soporte Móvil de Almacenamiento Informático removible, en gabinetes u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo, o bien asegurar con cable de bloqueo o algún otro medio que evite la sustracción no autorizada de las computadoras portátiles que se encuentren bajo su resguardo;

e) Verificar que las condiciones del lugar donde realiza sus labores sean las adecuadas para evitar que los recursos informáticos y la información bajo su resguardo puedan ser sustraídos por terceros no autorizados y en caso de no contar con las condiciones adecuadas informar a su Enlace

Informático;

f) Abstenerse de instalar software sin previa justificación, notificación y autorización de su Enlace Informático;

g) Solicitar a través del Enlace Informático el apoyo para desinstalar el software del que sospeche que tiene una anomalía;

h) Realizar respaldo de la Información Electrónica bajo su responsabilidad para la continuidad de sus funciones;

i) Reportar a su Enlace Informático correspondiente cualquier situación que considere que puede poner en riesgo el Ambiente de Seguridad Informática del Ente público.

2.- Todo Usuario de Activos Informáticos deberá cumplir las siguientes reglas de uso de contraseñas:

a) Mantener las contraseñas en secreto;

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas;

c) Seleccionar contraseñas de calidad, de acuerdo a las indicaciones informadas por el Responsable del Servicio de que se trate, y cuidando que:

c.1. Sean fáciles de recordar;

c.2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.;

c.3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos;

c.4. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas;

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas;

e) Cambiar las contraseñas provisionales en el primer inicio de sesión;

f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro;

g) Notificar directamente al responsable de apoyar la implementación y el seguimiento de las medidas de Seguridad Informática en su ámbito de competencia para cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad;

3.- El uso de recursos del personal o de terceros (Proveedores, Clientes, etc.) para el procesamiento de información en el lugar de trabajo debe ser controlado según el procedimiento de Seguridad Informática establecido y autorizado por el Enlace Informático responsable del área al que se destinen los recursos y verificarán que se cumplan medidas propuestas de Seguridad Informática de la presente norma.

4.- Todo Usuario que haga uso de equipo de cómputo o dispositivos móviles del Ente público debe atender

los Procedimientos de Seguridad de Equipos de Cómputo Portátil y Comunicaciones Móviles.

5.- Toda persona que desempeñe actividades para apoyar las funciones del ente público y que para sus tareas requiera hacer uso de activos informáticos del Ente público, tendrán las siguientes responsabilidades:

a) Asistir a los cursos de capacitación en materia de Seguridad Informática que brinde el ente público y que se determinen como obligatorios;

b) Establecer las medidas necesarias para proteger la información electrónica que se encuentre bajo su resguardo, conforme a la normatividad vigente;

c) Mantener activos y bajo la configuración asignada los sistemas de Seguridad Informática proporcionados por el ente público sobre los bienes, servicios e información a los que tenga acceso;

d) Realizar un respaldo de la Información electrónica bajo su responsabilidad al cambiar de: equipo asignado para el desempeño de sus actividades, de funciones, de área de adscripción o al finalizar su relación con el ente público, y entregarlo de manera formal a su jefe inmediato que haya estado encargado de supervisar sus funciones;

e) Quien se encuentre en el supuesto de la fracción anterior deberá eliminar del equipo toda la información electrónica institucional y en el caso de información electrónica sensible aplicar los procedimientos de borrado permanente que establezca el Ente público ;

f) Notificar a su Enlace Informático a través de su jefe inmediato cualquier cambio: de equipo, de funciones, o de área de adscripción para que se apliquen las medidas de Seguridad Informática correspondientes;

6.- El Enlace Informático deberá asegurar que todos los equipos que dejen de ser utilizados temporal o permanentemente no contengan información institucional, sean formateados y contengan solamente la imagen original del Sistema Operativo con que fueron adquiridos y que sea desinstalado todo el software que requiera del pago de licenciamiento por parte del Ente público;

7.- Toda persona que requiera retirar de las instalaciones del ente público algún equipo de cómputo o comunicaciones o software deberá contar con la autorización formal de su área administrativa correspondiente.

8.- Toda aplicación desarrollada por el Ente público o por un tercero debe tener un responsable único designado formalmente, de acuerdo a lo establecido en las políticas y normatividad institucional sobre desarrollo de sistemas informáticos.

9.- Todo Usuario de Recursos Informáticos y Usuario Externo deben de reportar los incidentes de seguridad a su jefe inmediato superior, al encargado del área donde presta su servicio o a la Mesa de Ayuda, tan pronto hayan tomado conocimiento de su ocurrencia.

10.- Los Usuario de Sistemas y Servicios Informáticos, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de Seguridad Informática, son responsables de registrar y comunicar inmediatamente las mismas a su Enlace Informático y Mesa de Ayuda correspondiente.

11.- El Usuario de Recursos Informáticos no debe realizar pruebas para detectar y/o utilizar una supuesta debilidad o falla de Seguridad Informática.

12.- Todo Usuario de Recursos Informáticos que detecte una anomalía de software en producción deberá:

a. Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

b. Alertar a su Enlace Informático correspondiente.

13.- El uso de recursos de los servidores públicos o usuario externo (proveedores, clientes, etc.) para el procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será controlado y autorizado por el Enlace Informático responsable del área al que se destinen los recursos y verificarán que se cumplan medidas propuestas de Seguridad Informática de la presente norma.

D.-. Ambiente de Seguridad Informática del ente público.

1.- Todo incidente o violación de la Seguridad Informática debe ser reportado al Área de Seguridad Informática a través de su Enlace Informático y Mesa de Ayuda para su investigación y resolución del incidente.

2.- Los responsables de servicios informáticos y los Enlaces Informáticos deberán apoyar la implementación de las medidas de control y acceso a las Áreas de Acceso Informático Restringido.

3.- El responsable de Seguridad Informática con el apoyo de los responsables del control de acceso a las Áreas de Acceso Informático Restringido deberá mantener un registro de dichas áreas en el que se identificarán la ubicación, las condiciones físicas, los activos informáticos a proteger y las medidas de protección física y lógicas aplicables.

4.- Los responsables del control de acceso a las Áreas de Acceso Informático Restringido deberán establecer las medidas de seguridad que deberán atender quienes accedan a ellas.

5.- El ingreso a las Áreas de Acceso Informático Restringido será autorizado en conjunto por el responsable del control de acceso a dichas áreas y al responsable de Seguridad Informática correspondiente.

6.- El ingreso o salida a las Áreas de Acceso Informático Restringido de equipos electrónicos, de cómputo, de almacenamiento, de comunicaciones, accesorios y otros dispositivos deberá ser autorizado por el responsable del control de acceso al área informática restringida y el responsable de Seguridad Informática y siempre deberán encontrarse relacionadas a un responsable de ellos que será la persona encargada de solicitar el movimiento.

7.- Cualquier persona que sea externa al Ente público no podrá acceder, ni permanecer en ninguna de las Áreas de Acceso Informático Restringido si no se encuentra acompañado de un servidor público ente público que también cuente con la autorización para su ingreso.

8.- Queda prohibido comer, beber y fumar dentro de cualquiera de las Áreas de Acceso Informático Restringido.

9.- Para cada área informática restringida el responsable de control de acceso deberá mantener un registro, que deberá hacer del conocimiento del responsable de la Seguridad Informática, de las personas autorizadas para acceder de manera temporal o permanente.

10.- Los responsables del control de acceso a las Áreas de Acceso Informático Restringido deberán mantener un registro de los accesos a los sitios bajo su responsabilidad en el que se identifique al menos el nombre de las personas autorizadas para su ingreso, la fecha y hora de entrada y salida, y de los equipos electrónicos: de cómputo, de almacenamiento, de comunicaciones, de accesorios y otros dispositivos que hayan ingresado y los motivos para su ingreso.

11.- Los responsables del control de acceso a las Áreas de Acceso Informático Restringido se encargarán de

vigilar que se realicen las acciones para mantener las condiciones físicas necesarias para proteger adecuadamente los recursos informáticos y la información electrónica que contengan.

12.- Los Enlaces Informáticos en conjunto con el área de recursos materiales de la Dirección de Administración serán responsables de vigilar que los bienes de cómputo y comunicaciones de su Unidad Administrativa que no se encuentren en uso sean ubicados en lugares físicos con las condiciones adecuadas para minimizar las posibilidades de sustracción, daño y deterioro.

13.- Los Enlaces Informáticos deberán verificar que los respaldos de información electrónica sensible se realicen bajo las condiciones de Seguridad Informática que se encuentren vigentes.

14.- El Responsable de Seguridad Informática debe verificar que los procedimientos de aprobación de Software incluyan aspectos para las aplicaciones de Gobierno Electrónico.

15.- Todo sistema de aplicación sensible a pérdidas potenciales y que requieran un tratamiento especial deben ejecutarse en una computadora dedicada (aislada) que solo debe compartir recursos con sistemas de aplicación confiable.

16.- Todo equipo de cómputo que lleve un registro de eventos debe mantener una sincronización de su reloj a de fin garantizar la exactitud de los registros de auditoría.

17.- Los Sistemas Multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

18.- Toda aplicación que envíe mensajes que contengan información clasificada, debe utilizar controles criptográficos para que los mensajes sean enviados en forma cifrada.

19.- . Toda aplicación que transmita información clasificada fuera del Ente público debe manejar la información cifrada.

20.- Establecer mecanismos de no Repudio para resolver disputas acerca de la ocurrencia de un evento o acción.

21.- Todas las claves criptográficas deben ser protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

22.- Todo el equipamiento que se utilice para generar, almacenar y archivar claves debe ser considerado crítico y de alto riesgo.

23.- Para evitar exponer información utilizando algunos canales ocultos y código malicioso de medios indirectos el Responsable del Servicio debe:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.

b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

c) Controlar el acceso y las modificaciones al código instalado.

d) Utilizar herramientas para la protección contra la infección del software con código malicioso.

24.- Para todo desarrollo de software realizado por terceros se deben establecer:

a) Acuerdos de licencias, propiedad de código y derechos conferidos;

b) Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso

de quiebra de la tercera parte;

c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.;

d) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías, y;

e) Verificar el cumplimiento de las condiciones de seguridad contempladas.

25.- Todo plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo.

E.- Seguridad de los Servicios Informáticos del ente público.

1.- Los responsables de servicios informáticos deberán mantener actualizados, configurados y en operación los equipos, accesorios y software relacionado con sus servicios atendiendo las recomendaciones de los fabricantes, proveedores e indicaciones del responsable de Seguridad Informática.

2.- Los responsables de servicio serán encargados de:

a) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales como: robo o hurto, incendio, explosivos, humo, inundaciones o filtraciones de agua (o falta de suministro, polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión), radiación electromagnética, derrumbes, etc.;

b) Administrar las contraseñas de acuerdo al procedimiento de gestión de contraseñas;

c) Aislar de las inclemencias ambientales (temperatura, humedad, etc.) los elementos que requieren protección especial para reducir el nivel general de protección requerida;

d) Almacenar la documentación del sistema en forma segura y restringir el acceso a la documentación del sistema al personal autorizado por el responsable de la Información;

e) Asegurar la disponibilidad del equipo informático mediante un programa permanente de mantenimiento preventivo;

f) Asignar los privilegios a los usuarios de acuerdo a la solicitud y aprobación del Enlace Informático y solicitar a intervalos regulares una revisión de derechos de accesos de los usuarios;

g) Atender las medidas y recomendaciones que se acuerden con el responsable de la Seguridad Informática;

h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron su perfil, o de aquellos a los que se les revocó la autorización, se desvincularon del Ente público o sufrieron la pérdida/robo de sus credenciales de acceso previa notificación del Enlace Informático del área de su adscripción;

i) Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar;

j) Controlar el acceso lógico a los servicios, tanto a su uso como a su administración;

k) Documentar y mantener actualizados los procedimientos operativos de los sistemas de Información Electrónica;

l) Efectuar el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados tomando en cuenta los nuevos requerimientos de los sistemas así como las tendencias actuales proyectadas en el procesamiento de la información del Ente público para el período estipulado de la vida útil de cada componente;

m) Efectuar revisiones periódicas de registro de usuarios con el objeto de:

m.1 Cancelar identificadores y cuentas de usuario redundantes;
m.2 Inhabilitar cuentas inactivas por más de 60 días naturales, y
m.3 Eliminar cuentas inactivas por más de 120 días naturales;

n) En coordinación con los Enlaces Informáticos y el responsable de Seguridad Informática realizar ejercicios de análisis de riesgos a fin de garantizar la continuidad de los servicios y contribuir al Sistema de Seguridad de la Información;

o) Establecer en coordinación con el responsable de Seguridad Informática los procedimientos para asegurar la continuidad operativa y la recuperación del servicio e información en caso de eventualidades o desastres;

p) Establecer los controles de acceso a las aplicaciones, contemplando al menos los siguientes aspectos:

p.1 Identificar los requerimientos de seguridad de cada una de las aplicaciones.
p.2 Identificar toda la Información relacionada con las aplicaciones.
p.3 Definir los perfiles de acceso de Usuarios estándar, comunes a cada categoría de puestos de trabajo.
p.4 Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles;

q) Establecer medidas para monitorear el funcionamiento del servicio y detectar de manera oportuna aquellos incidentes que pudieran afectar de alguna forma al desempeño, disponibilidad, confiabilidad, entre otro:

q.1 Identificar los controles de prevención, detección y corrección;

q.2 Instalar periódicamente las actualizaciones de seguridad;

q.3 Implementar procedimientos para la administración de medios informáticos removibles, considerando:

1. Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Ente público.
2. Requerir autorización para retirar cualquier medio del Ente público y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
3. Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

r) Mantener instalados y habilitados sólo aquellos servicios que sean utilizados;

s) Mantener el registro de los incidentes que hayan afectado de alguna forma al desempeño, disponibilidad, confiabilidad, etc. Identificando al menos: la causa, el ente que lo originó (al mayor nivel de precisión que sea posible), el nivel de gravedad, los alcances, los efectos percibidos, la

solución adoptada y las medidas establecidas para minimizar la posibilidad de que vuelva a presentarse;

t) Mantener el registro de los usuarios autorizados para hacer uso del servicio identificando para cada uno de ellos, al menos: la vigencia de la autorización, los permisos y restricciones con respecto al servicio y el estado para su acceso (por ejemplo: activo, cancelado, inactivo, etc.);

u) Mantener restringido y protegido el acceso a la información institucional que sea manejada por el servicio del que son responsables, atendiendo a las indicaciones de Seguridad Informática; a los lineamientos emitidos por el ente público y a la normatividad que establezca el área responsable de la Seguridad de la Información;

v) Otorgar al usuario los privilegios mínimos necesarios para desarrollar su trabajo, en consecuencia, si existiera algún servicio especial para el desarrollo de sus funciones debe de tramitarlo con su Enlace Informático;

w) Otorgar el acceso a los recursos, funciones y servicios informáticos sólo hasta que se hayan completado los procedimientos formales de autorización de acuerdo a la normatividad vigente;

x) Registrar, documentar y comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones con la finalidad de que sean utilizadas para tomar medidas correctivas;

y) Registrar las actividades realizadas en la operación de sistemas y servicios informáticos;

z) Registrar y monitorear aquellos eventos que consideren críticos para la operación que se encuentra bajo su responsabilidad;

aa) Revisar los registros de auditoría con la finalidad de producir un informe de las amenazas detectadas contra los sistemas, para realizar un análisis de riesgos.

bb) Ubicar el equipamiento crítico para proporcionar el servicio en las Áreas de Acceso Informático Restringido;

I. Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo Servidor Público. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas; y

3.- El Responsable del Servicio Infraestructura Electromecánica debe:

a) Contar con al menos un equipo portátil de combate y extinción de incendios para hacer frente a cualquier eventualidad que se pueda presentar.

b) Contar con el suministro de energía eléctrica ininterrumpible para garantizar la continuidad del servicio a la infraestructura de cómputo y comunicaciones que soporta las operaciones informáticas críticas del Ente público;

c) Instalar una planta generadora de energía eléctrica de respaldo para mantener la continuidad del suministro eléctrico en caso de falla o falta de suministro por parte de la compañía encargada de proporcionarla

d) Disponer del suficiente suministro de combustible para garantizar que la planta generadora de energía eléctrica pueda funcionar por un período prolongado;

e) Implementar protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las disposiciones normativas vigentes,

f) Proporcionar las condiciones de temperatura y humedad relativa en los centros de procesamiento de datos a fin de garantizar el ambiente de Tecnologías Informáticas (TI) adecuado para la operación del equipamiento de cómputo y comunicaciones;

g) Proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía;

h) Verificar la distribución de tomas de energía eléctrica necesarias así como de líneas de suministro para evitar en la medida de lo posible un único punto de falla en el suministro de energía;

i) Verificar que las plantas generadoras de energía eléctrica sean inspeccionadas y probadas periódicamente para asegurar que funcionen adecuadamente;

j) Verificar que los equipos de energía ininterrumpible sean inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que cuentan con el tiempo de respaldo requerido; y

4.- El Responsable de la Gestión de Control de Cambios debe:

a) Controlar que los cambios en los componentes operativos y de comunicaciones no afecten a la seguridad de los mismos ni de la información que soportan;

b) Establecer los criterios de aprobación para nuevos Sistemas de Información, actualizaciones y nuevas versiones del mismo, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva;

c) Evaluar y registrar previamente todo cambio de operaciones en cuanto a aspectos técnicos y de Seguridad Informática, mediante el Procedimiento de Control de Cambios;

d) Evaluar el posible impacto operativo de los cambios previstos y verificar su correcta implementación;

e) Registrar toda la información relevante de cada cambio implementado; y

5.- El Responsable de Desarrollo de Sistemas debe:

a) Administrar todos los programas fuentes;

b) Asegurar que todo programa ejecutable en producción tenga un único programa fuente asociado que garantice su origen;

c) Asegurar que todo cambio a realizar en el software de aplicación debe efectuarse en el ambiente de desarrollo;

d) Asegurar que para cada cambio realizado en el software de aplicación deben actualizarse los respectivos cambios en el manual de usuario y en la documentación operativa;

e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación;

f) Contar con un control que permita determinar las responsabilidades del personal involucrado en el proceso de entrada de datos;

g) Definir Responsables de la Información para cada uno de los ambientes de procesamiento existentes;

h) Definir un procedimiento, para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar los riesgos de fallas de procesamiento y vicios por procesos de errores;

i) Determinar, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados;

j) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios;

k) Elaborar una evaluación de riesgos antes de diseñar la aplicación con el objeto de definir los requerimientos de seguridad e identificar los controles apropiados a aplicar en las etapas del desarrollo de sistemas, prueba de las aplicaciones y ambiente de producción;

l) Establecer procedimientos para validar la salida de los datos de las aplicaciones;

m) Identificar y documentar claramente la sensibilidad de la aplicación;

n) Identificar y acordar con el Administrador de la Aplicación sensible cuando la aplicación deba de ejecutarse en un ambiente compartido y las aplicaciones con las que compartirá los recursos;

o) Impedir el acceso a los compiladores, editores y otras utilerías del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo;

p) Implementar controles que aseguren la validez de los datos introducidos;

q) Incluir controles de seguridad y registros de auditoría con el objeto de evitar la pérdida, modificación o uso inadecuado de los datos en los Sistemas de Información;

r) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operación;

s) Llevar un registro actualizado de todos los programas fuentes en uso, indicando el nombre del programa, programador, analista del programa, versión, fecha de última modificación, fecha/hora de compilación y estado (en modificación, en producción).

t) Respaldar en medios seguros la última, penúltima y antepenúltima versión de los programas fuente y ejecutables así como su documentación de entorno de cada aplicación como medida de prevención para cualquier contingencia;

u) Restringir el acceso a la información por fuera del sistema para evitar la modificación directa del dato almacenado, la excepción de uso de las aplicaciones para actualización o eliminación de Información Electrónica se debe realizar a través de una solicitud formal previa autorización del Responsable de la Información;

v) Separar las actividades y ambientes de las áreas de desarrollo, pruebas y producción en entornos diferentes;

w) Toda actualización realizada a las aplicaciones debe ser registrada;

x) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los Usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión;

y) Utilizar técnicas criptográficas apropiadas que permitan la protección de la confidencialidad e integridad de la información cuando se utilice información sensible.

z) Verificar que todo sistema desarrollado e instalado al interior del Ente público y puesto en producción generen registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad;

aa) Verificar que los registros de auditoría sean archivados preferentemente en un equipo diferente al que los genere.

bb) Verificar que todo cambio a realizar en las aplicaciones sea propuesto por Usuarios autorizados, que tenga la aprobación del Responsable del Sistema de la Información y que no se violen los requerimientos de Seguridad Informática; y

6.- El Responsable del Almacenamiento y Respaldo de Información está obligado a:

a) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal;

b) Determinar los requerimientos para resguardar una copia de cada software o dato en función de su criticidad;

c) Disponer y controlar la realización de copias de respaldo;

d) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo; una vez concluida la posibilidad de ser reutilizados y asegurar la destrucción de los medios desechados;

e) Extender los mismos controles de seguridad aplicados a los dispositivos en el sitio principal al sitio de resguardo;

f) Probar periódicamente los sistemas de resguardo, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del Ente público;

g) Retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el Ente público, y

7.- El responsable de la gestión de redes debe de:

a) Autenticar la conexión de nodos de los Sistemas Informáticos;

b) Definir procedimientos para solicitar y aprobar accesos a Internet;

c) Establecer un programa de:

c.1 Control de cambios (etiquetado, documentación, control de activos);
c.2 Control de red (diagramas), y
c.3 Mantenimiento.

d) Implementar controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Ente público, contra el acceso no autorizado;

e) Implementar controles para limitar la capacidad de los entornos de conexión de los Usuarios:

e.1 Correo electrónico;
e.2 Transferencia de archivos (FTP);
e.3 Acceso interactivo. (Terminal Remota);
e.4 Acceso a la red fuera del horario laboral. (VPN, RAS, etc.),

f) Incorporar controles de ruteo que verifiquen la dirección de origen y destino, para asegurar que las conexiones informáticas y los flujos de información no violen los Controles de Acceso.

g) Proteger el cableado que transporta datos o soporta servicios de información contra posibles intercepciones o daños;

h) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados;

i) Proteger las conexiones realizadas en los puertos de diagnóstico y configuración remota;

j) Registrar los accesos de los Usuarios a Internet con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares;

k) Realizar una evaluación de riesgos para la autenticación de usuarios que requieren conexiones externas al Ente público;

l) Separar los cables de energía de los cables de comunicaciones para evitar interferencias;

m) Subdividir la red en dominios lógicos separados con el objeto de controlar la seguridad de la red Institucional;

n) Verificar que las áreas en los puntos terminales y de inspección tengan cerradura;

o) Utilizar piso falso, canaleta o cableado oculto en la pared, siempre que sea posible, cuando corresponda a las Instalaciones de Procesamiento de información;

p) Verificar que el cableado cumpla con los requisitos técnicos vigentes de las Normas Mexicanas; y

8.- El responsable de la mensajería electrónica debe:

a) Proteger contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.;

b) Proteger los archivos adjuntos de correo electrónico;

c) Usar de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos;

d) Instrumentar controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados;

e) Establecer aspectos operativos para garantizar el correcto funcionamiento del servicio (ejemplo: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del Usuario, etc.);

9.- El responsable del sistema operativo debe:

a) Asegurar que toda actualización que deba realizarse en el sistema operativo debe ser probada en equipos piloto por el Responsable del Servicio Informático a fin de garantizar que no se produzcan impactos negativos en su funcionamiento y Seguridad Informática;

b) Limitar y controlar el uso de utilerías del sistema operativo;

c) Realizar una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo;

d) Utilizar la Norma de Nomenclatura de Equipos de Cómputo y Servidores para la identificación de los equipos de cómputo ubicada en el sitio de normas informáticas en la intranet; y

10.- El responsable de los archivos del sistema debe:

a) Controlar el acceso a los archivos del sistema de manera segura; y

11.- El responsable de procesamiento y control de la producción debe de:

a) Asegurar que todo programa en producción cuente con su manual de operación.

b) Controlar que no se de mantenimiento de programas en el ambiente de producción;

c) Resguardar todos los programas ejecutables en el ambiente de producción; y

12.- El responsable de pruebas de sistemas debe:

Realizar las pruebas con una copia de datos extraídos del ambiente operativo y una vez terminada la prueba se debe borrar su contenido.

VI.-Sanciones.

El incumplimiento de las disposiciones establecidas en estas Políticas serán objeto de sanción administrativa en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, independientemente de las sanciones de las que pudieran hacerse acreedores en términos de las demás disposiciones jurídicas aplicables.