POLÍTICAS O LINEAMIENTOS PARA LA GESTIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

ORGANO DE CONTROL Y EVALUACIÓN GUBERNAMENTAL.

H. AYUNTAMIENTO DE SANTA ANA, SONORA.

Contraloría Municipal
Santa Ana, Sonora

Índice

Indice

A.-

Contraloría Municipal
Santa Ana, Sonora

POLITICAS PARA LA SEGURIDAD INFORMATICA

Órgano de Control y Evaluación Gubernamental

I.- Introducción. -

La Seguridad informática tiene una especial importancia para cualquier persona que realiza sus actividades diarias con las Tecnológicas de la Información y la Comunicación. Saber manejar estos recursos ayuda a optimizar la seguridad informática y la confianza de los que usan estos medios, esto, solo se logra a través de una protección de los elementos que integran dichas tecnologías y que administran, procesan e intercambian información.

A través de los años estas tecnologías han sufrido incontable número de actualizaciones y esto modifica el riesgo de la información en los sistemas y también implica la aparición de nuevos riesgos y así aumentan las amenazas en el robo de información. Esto, ha motivado a este Órgano de Control y Evaluación Gubernamental a desarrollar políticas para protección de la información que se avocan principalmente en el uso adecuado de estas tecnologías y mejorar la prevención de riesgos informáticos.

Es por esto que las presentes Políticas se plantean como una herramienta de organización para unir esfuerzos y crear conciencia entre el personal administrativo y de servicios de este Ayuntamiento y así poder estar protegidos ante cualquier amenaza informática. En este documento se plantea una política de Seguridad Informática que demanda un alto compromiso con este Ayuntamiento, perspicacia técnica para crear fortalezas y descubrir debilidades en su aplicación, y perseverancia para conservarla actualizada de forma continua en función de los cambios tecnológicos que la influyen.

El Órgano de Control y Evaluación Gubernamental emite esta normatividad con fundamento en el Artículo 164, Fracción XX, del Reglamento Interior del H. Ayuntamiento de Santa Ana, que le facultan para elaborar los lineamientos generales para la formulación de los manuales de organización y procedimientos al que habrán de sujetarse las dependencias y entidades municipales, los cuales deberán ser aprobados por el Ayuntamiento.

Contraloría Municipal
Santa Ana, Sonora

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 Instituto;

II. **Ambiente de Seguridad Informática:** Medidas de Seguridad Informática que se establecen en el Ayuntamiento, con la finalidad de proteger sus activos informáticos, crear conciencia de la seguridad, aumentar el compromiso de su personal y garantizar la continuidad de las actividades de este Ayuntamiento.

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 Empleado y el Ayuntamiento.

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. **OCEG:** Órgano de Control y Evaluación Gubernamental.

Contraloría Municipal
Santa Ana, Sonora

XIII. **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 Instituto;

XIV. **Enlace Informático**: el servidor público designado por el Titular de cada Unidad Administrativa, como responsable para apoyar y acordar con el Órgano de Control y Evaluación Gubernamental todo lo relacionado con la coordinación de la función informática al interior de la Unidad Administrativa de su adscripción;

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

XVI. **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 H. Ayuntamiento de Santa Ana.

XVII. **Información electrónica sensible**: la información en formato electrónico o asimilable directamente a través de un recurso informático que sea valiosa para este Ayuntamiento 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 de este Ayuntamiento, la consecución de sus objetivos, o el cumplimiento de la normatividad vigente;

XVIII. **Ayuntamiento**: El H. Ayuntamiento de Santa Ana Sonora

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

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

XXI. **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;

XXII. **Planes de continuidad:** es la planificación que identifica el Instituto ante la exposición de amenazas internas y externas que ofrecen una prevención de recuperación de las operaciones del Ayuntamiento, manteniendo la integridad del sistema.

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

XXIV. **Políticas:** Políticas para la Seguridad Informática del H. Ayuntamiento de Santa Ana.

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

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

XXVII. **Usuario Externo:** A la persona externa (Consultores, Soporte de Hardware, software, servicio social, estadías, Prácticas profesionales, etc.) al Instituto que haga uso de bienes, servicios, recursos informáticos o de información electrónica que sea responsabilidad del Ayuntamiento.

Contraloría Municipal
Santa Ana, Sonora

III-. Objeto. -

Instituir la política institucional en materia de Seguridad Informática que apoye la Seguridad de la Información, entendida como la conservación de su integridad, confidencialidad y disponibilidad, así como organizar y regular acciones para disminuir daños a la infraestructura tecnológica y a los sistemas informáticos.

IV.- Marco Jurídico. -

a) Constitución Política de los Estados Unidos Mexicanos.

b) Leyes.

1. Ley de Gobierno y Administración Municipal
2. Ley Federal de Protección de Datos Personales;
3. Ley Federal del Derecho de Autor;
4. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
5. Ley Estatal de Responsabilidades Administrativas de los Servidores Públicos, y
6. Código Penal Federal.

c) Reglamentos.

1. Reglamento Interior del H. Ayuntamiento de Santa Ana.

Contraloría Municipal
Santa Ana, Sonora

V.- Políticas Generales. -

A.- Organización de la Seguridad Informática.-

1.- El objetivo principal de la Seguridad Informática será resguardar desde el ámbito tecnológico la información electrónica institucional, los recursos informáticos y los servicios tecnológicos necesarios para que el H. Ayuntamiento de Santa Ana pueda desempeñar sus funciones y obligaciones que le correspondan de acuerdo a la normatividad aplicable.

2.- La Seguridad Informática en el H. Ayuntamiento de Santa Ana involucra una responsabilidad a cargo de los administradores y usuarios de Usuario de Sistemas y Servicios Informáticos Institucionales.

3.- La Contraloría Municipal es el área responsable de coordinar acciones; establecer la plataforma tecnológica; y constituir lineamientos, estándares, criterios, medidas y otras disposiciones técnicas, en materia de Seguridad Informática.

4.- El Titular del Órgano de Control y Evaluación Gubernamental designará a un Coordinador y a un Responsable de la Seguridad Informática del H. Ayuntamiento de Santa Ana quienes le apoyarán con las labores relacionadas con la Seguridad Informática del mismo.

5.- El Coordinador de Seguridad Informática del H. Ayuntamiento de Santa Ana tendrá las siguientes facultades:

a) Proponer e integrar estrategias y elementos para conformar el Programa Institucional de Seguridad Informática ordenados al Sistema de Seguridad de la Información, en coordinación con el Titular del Órgano de Control y Evaluación Gubernamental, los Enlaces Informáticos y los Directores de Área.

b) Coordinar los procesos y proyectos en materia de Seguridad Informática con los Enlaces Informáticos, los Directores de Área y con el Responsable de Seguridad Informática del Ayuntamiento.

c) Conservar 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 Ayuntamiento.

d) Instituir acuerdos en materia de Seguridad Informática con áreas internas e instituciones externas al Ayuntamiento.

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

f) Presentar criterios en materia de Seguridad Informática para la clasificación, registro y protección de los recursos informáticos del Ayuntamiento.

Contraloría Municipal
Santa Ana, Sonora

g) Publicar en el portal de Transparencia Municipal los documentos normativos en materia de Seguridad Informática emitidos por el Titular del Órgano de Control y Evaluación Gubernamental y;

h) Las demás que determine el Titular del Órgano de Control y Evaluación Gubernamental.

6.- El Responsable de la Seguridad Informática del Ayuntamiento, será el encargado de:

I. Coordinar con los Enlaces Informáticos y los responsables de servicio las acciones en materia de Seguridad Informática que deberán llevarse a cabo en el Ayuntamiento.

II. Exponer políticas y especificaciones técnicas de bienes y servicios, procedimientos, acciones y medidas específicas en materia de Seguridad Informática al Titular del Órgano de Control y Evaluación Gubernamental; que sean aplicables a cualquiera de los elementos tecnológicos que constituyan la plataforma de Seguridad Informática del Ayuntamiento.

III. Mantener la administración del sistema de autentificación de usuarios que permite el acceso a los recursos y servicios informáticos y de comunicaciones del Ayuntamiento.

IV. 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 Ayuntamiento;

V. Del sistema de gestión de incidentes de seguridad de la información, examinar aquellos que involucren los servicios informáticos a fin de establecer controles para descubrir, corregir y prevenir incidentes posteriores.

VI. 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;

VII. Proponer la plataforma tecnológica para el soporte del ambiente de Seguridad Informática del Ayuntamiento;

VIII. Mantener actualizado el inventario de Activos Informáticos relacionados con la Plataforma de Seguridad Informática del Ayuntamiento como complemento del inventario de activos de Información;

IX. Realizar exámenes selectivos a los controles de los activos informáticos para certificar que se mantenga sobre ellos la aplicación de las recomendaciones y lineamientos en materia de Seguridad Informática;

X. 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;

Contraloría Municipal
Santa Ana, Sonora

XI. Publicar en las páginas oficiales los documentos técnicos en materia de Seguridad Informática emitidos por el Órgano de Control y Evaluación Gubernamental.

XII. Promover el cumplimiento de la normatividad informática en el Ayuntamiento;

XIII. Especificar controles de detección y prevención para la protección contra software malicioso;

XIV. Efectuar controles para la protección contra software malicioso en la infraestructura de cómputo y telecomunicaciones;

XV. Delimitar las cuentas de acceso para la administración de los equipos de cómputo para resguardar la configuración de los mismos, las cuales hará del conocimiento a los Enlaces Informáticos;

XVI. Examinar los registros de eventos de los diferentes equipos que formen parte del ambiente de seguridad del Ayuntamiento a fin de colaborar con el responsable del servicio en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad;

XVII. Recopilar y administrar las claves criptográficas incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados;

XVIII. Revocar las claves criptográficas, cuando las claves estén comprometidas o cuando un usuario que haga uso de ellas se desvincule del Ayuntamiento.

XIX. Recuperar las claves pérdidas o alteradas como parte de la administración para su continuidad;

XX. Coordinar, administrar y registrar todos los nombres de equipos y dominios que son accesibles en la Internet del Ayuntamiento;

XXI. Inspeccionar y registrar todos los certificados de seguridad de los sitios del Ayuntamiento;

XXII. Sistematizar los grupos de reacción inmediata y otros grupos de trabajo para manejar los reportes de incidentes y anomalías de Seguridad Informática;

XXIII. 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

XXIV. Las demás que determine el Titular del Órgano de Control y Evaluación Gubernamental.

7.- Para facilitar las tareas de planeación y coordinación de la Seguridad Informática se instituye un Grupo Institucional de Seguridad Informática integrado por el Titular del Órgano de Control y Evaluación Gubernamental, el Responsable de Seguridad Informática, los Directores de Área y los Enlaces Informáticos.

8.- El Grupo Institucional de Seguridad Informática será coordinado por el Titular del OCEG y tendrá como secretario técnico al Responsable de la Seguridad Informática; los demás miembros serán considerados como vocales.

9.- Cada miembro del Grupo Institucional de Seguridad Informática tendrá derecho a voz y voto y en caso de empate el voto del Coordinador del Grupo será considerado como voto de calidad.

10.- El Grupo Institucional de Seguridad Informática tendrá las siguientes funciones:

a) Realizar ejercicios de análisis de riesgos de acuerdo a la metodología establecida en el Sistema de Seguridad de la Información;

b) Elaborar y dar seguimiento de los Planes de Continuidad que van a ejecutar el Grupo de Operación de Seguridad Informática;

c) Ratificar las medidas generales de Seguridad Informática;

d) Ratificar el Programa Institucional de Seguridad Informática;

e) Ratificar estrategias en materia de Seguridad Informática;

f) Coordinar al Grupo de Operación de Seguridad Informática;

g) Establecer el listado de Activos Informáticos relacionados con la plataforma de Seguridad Informática;

h) Ratificar la plataforma tecnológica para sustentar el ambiente de Seguridad Informática;

i) Elegir los responsables de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática;

j) Elegir las Áreas de Acceso Informático Restringido y a los responsables de controlar su acceso;

k) Valorar el desempeño del ambiente de Seguridad Informática;

l) Ejecutar propuestas para mejorar el ambiente de Seguridad Informática; y

m) Las demás que determine el Titular del Órgano de Control y Evaluación Gubernamental

11.- Para facilitar la ejecución y puesta en práctica de las tareas, acciones y medidas en materia de Seguridad Informática establecidas por el Grupo Institucional de Seguridad Informática se crea el Grupo de Operación de la Seguridad Informática que estará conformado por el Responsable de la Seguridad Informática y por los responsables de los servicios informáticos del Ayuntamiento.

Contraloría Municipal
Santa Ana, Sonora

12.- El Grupo de Operación de la Seguridad Informática será coordinado por el responsable de la Seguridad Informática quien elegirá un Secretario Técnico para que le asista en las tareas relacionadas con la coordinación y seguimiento del grupo.

13.- El Grupo de Operación de la Seguridad Informática tendrá las siguientes funciones:

a) Efectuar y poner en práctica las medidas acordadas por el Grupo Institucional de Seguridad Informática;

b) Dar seguimiento al cumplimiento del Programa Institucional de Seguridad Informática;

c) Mantener un sistema de monitoreo y seguimiento del desempeño del ambiente de Seguridad Informática;

d) Ejecutar estudios y propuestas para optimizar el desempeño del ambiente de Seguridad Informática;

e) Apoyar en el diseño y modificaciones de la plataforma tecnológica que soporta al ambiente de Seguridad Informática;

f) Convenir acciones técnicas tendientes a optimizar el desempeño del ambiente de Seguridad Informática;

g) Instituir grupos de trabajo específico para examinar en conjunto con los Responsables de la Información Electrónica Institucional, los riesgos de los accesos de terceros a la información del Ayuntamiento y proponer medidas con el propósito de minimizar sus posibles efectos;

h) Presentar a los responsables de cada uno de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática del Ayuntamiento.

i) Instituir grupos de reacción inmediata para la vigilancia de emergencias en materia de Seguridad Informática;

j) Crear medidas para el control de acceso físico y lógico a las áreas designadas como de acceso restringido;

k) Constituir el programa de ejercicios de análisis de riesgos de los activos informáticos que deberán ejecutar los responsables de servicios y los enlaces informáticos, para avalar su continuidad y para auxiliar al Sistema de Seguridad de la Información para este fin;

l) Elaborar e poner en practica Planes de Continuidad necesarios para atender eventualidades que puedan afectar la continuidad de las actividades del Ayuntamiento.

m) Coordinar las tareas definidas en los Planes de Continuidad;

n) Hacer ensayos, mantenimiento y reevaluación de los Planes de Continuidad;

o) Dar a conocer al personal implicado todo cambio realizado al plan de contingencia;

p) Instaurar los procedimientos, requerimientos y medidas que deberán atender los responsables, administradores y usuarios de servicios informáticos para utilizar los recursos tecnológicos que sean responsabilidad del Ayuntamiento; y

q) Las demás que determine el Grupo Institucional de Seguridad Informática.

14.- Los Enlaces Informáticos tendrán las siguientes responsabilidades con respecto a la Seguridad Informática en el Ayuntamiento:

a) Atender las disposiciones en materia de Seguridad Informática que se expongan en el Ayuntamiento y promover el acatamiento 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, ejecutar ejercicios de análisis de riesgos que contribuyan a la continuidad operativa de los Servicios Informáticos y de Seguridad de la Información;

d) Facilitar información sobre los registros de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática del Ayuntamiento que se encuentren asignados a su Unidad Administrativa;

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

f) Comprobar las condiciones del Ambiente de Seguridad Informática de su Unidad Administrativa y proponer al Grupo Institucional de Seguridad Informática medidas para mejorarlo;

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

h) Aquellas adicionales que determine el Grupo Institucional de Seguridad Informática.

Contraloría Municipal
Santa Ana, Sonora

B.- 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 presentadas por el Ayuntamiento que se encuentren publicadas en la internet institucional.

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

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 seguridad;

e) Comprobar 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) Requerir a través del Responsable del Seguridad informática el apoyo para desinstalar el software del que sospeche que tiene una anomalía;

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

i) Reportar al Responsable de Seguridad informática y a su Enlace Informático correspondiente cualquier situación que considere que puede poner en riesgo el Ambiente de Seguridad Informática del Ayuntamiento.

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

a) Proteger las contraseñas en secreto;

b) Solicitar 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:

1. Sean fáciles de recordar;

2. No estén apoyadas 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.;

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

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

d) Cambiar las contraseñas temporales en el primer inicio de sesión;

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

f) Comunicar 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 vigilado según el procedimiento de Seguridad Informática instituido y autorizado por el Enlace Informático responsable del área al que se consignen los recursos y comprobarán 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 Ayuntamiento 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 Ayuntamiento y que para sus tareas requiera hacer uso de activos informáticos del mismo, tendrán las siguientes responsabilidades:

a) Asistir a los cursos de capacitación en materia de Seguridad Informática que ofrezca el Ayuntamiento y que el Grupo Institucional de Seguridad Informática determine como obligatorios;

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

c) Mantener activos y bajo la configuración asignada los sisternas de Seguridad Informática proporcionados por el Ayuntamiento 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 Ayuntamiento, 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 emplear los procedimientos de borrado permanente que establezca el Ayuntamiento.

6.- El Responsable de Seguridad informática 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 Ayuntamiento;

7.- Toda persona que requiera retirar de las instalaciones del Ayuntamiento 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 Ayuntmaiento 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 al Responsable de Seguridad Informatica tan pronto hayan tomado conocimiento de su ocurrencia.

10.- 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 causar nuevas vulnerabilidades. En consecuencia, su uso será controlado y acreditado por el Enlace Informático responsable del área al que se destinen los recursos y comprobarán que se cumplan medidas propuestas de Seguridad Informática de la presente norma.

Contraloria Municipal
Santa Ana, Sonora

C.-. Ambiente de Seguridad Informática del Ayuntamiento

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

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

3.- El responsable de Seguridad Informática 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.- El Responsable de la Seguridad Informatica 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 acreditado por 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 Ayuntamiento no podrá acceder, ni permanecer en ninguna de las Áreas de Acceso Informático Restringido si no se encuentra acompañado de un servidor público del Ayuntamiento 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.

Contraloría Municipal
Santa Ana, Sonora

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

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

11.- 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 confidencial.

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

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

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

15.- . Toda aplicación que transmita información clasificada fuera del Ayuntamiento debe manejar la información cifrada.

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

Contraloría Municipal
Santa Ana, Sonora

VI.-Sanciones. -

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

Transitorios

Primero. Las presentes políticas entraran en vigor a partir de su publicación en la página oficial de este Ayuntamiento y en el periódico mural del mismo.

El presente documento fue emitido por el Titular del Órgano de Control y Evaluación Gubernamental. Blas Martin Méndez Zazueta el 30 de Septiembre de 2020.

ULTIMA HOJA DE LAS POLÍTICAS O LINEAMIENTOS PARA LA GESTIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EMITIDA POR EL TITULAR DEL ORGANO DE CONTROL Y EVALUACIÓN GUBERNAMENTALL EL DÍA 30 DE SEPTIEMBRE DE 2020 Y PUBLICADAS EN LA PAGINA OFICIAL DEL H. AYUNTAMIENTO DE SANTA ANA EL DÍA 10 DE OCTUBRE DE 2020, MISMAS QUE SE HACEN CONSTAR DE 21 FOJAS UTILES, LO ANTERIOR EN CUMPLIMIENTO A LO DISPUESTO POR EL ARTICULO 164, FRACCIÓN XX, DEL REGLAMENTO INTERIOR DEL H. AYUNTAMIENTO DE SANTA ANA.

El Titular de Órgano de Control y Evaluación Gubernamental

Lic. Blas Martin Méndez Zazueta

Contraloria Municipal
Santa Ana, Sonora