Coordinación de Control Interno Organismo Operador Parque Solidaridad

Lineamientos para la Seguridad Informática en el Organismo Operador del Parque de la Solidaridad.

Fecha de elaboración: 25/10/17 Fecha de actualización: 25/10/17

Elaboro	Reviso	Aprobó
Francisco Javier Lozano García	Felipe de Jesús Lozano Padilla	José Ascensión Velázquez Hernández

Se expiden los presentes Lineamientos en la Ciudad de Guadalajara Jalisco a los veinticinco días del mes de octubre de dos mil diecisiete.

Lineamientos para la Seguridad Informática en el Organismo Operador del Parque de la Solidaridad.

1. OBJETIVO

Establecer disposiciones administrativas y legales para la Seguridad Informática en el Organismo Operador del Parque de la Solidaridad.

2. ALCANCE

Los presentes Lineamientos para la asignación y uso de los Sistemas de Información, son de observancia obligatoria para todos los Servidores Públicos del Organismo Operador del Parque de la Solidaridad.

3. DEFINICIONES

Artículo 1.-Para efectos de los presentes Lineamientos se deberá entender por:

Antivirus.- Software especializado diseñado para detectar, eliminar y prevenir virus informáticos en los dispositivos de la Red;

Aplicación.- Cualquier programa computacional de uso específico para el Organismo que se encuentre en operación y que puedan desarrollarse de manera interna por servidores/as públicos/as especializados/as, por terceros de manera particular para el Organismo o ser licenciadas por uno o varios proveedores contratados para tal efecto;

Organismo.- El Organismo Operador del Parque de la Solidaridad;

Cadenas.- Término usado para referirse a mensajes de Correo Electrónico que son enviados a más de tres personas y cuyo contenido no es laboral;

Confidencialidad.- Es aquella por medio de la cual se garantiza que determinada información está accesible únicamente a servidores públicos autorizados de la gestión de la información y es una de las piedras angulares de la seguridad informática;

Correo Electrónico.- Servicio de la Red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos;

Contraseña.- Palabra clave mediante la cual el Servidor Público, puede tener acceso a una aplicación, sistema de información o elemento de infraestructura básico;

Dirección.- Dirección General;

Equipo de Cómputo.- Dispositivo electrónico de uso personal capaz de almacenar información, procesar datos y entregarle a el Servidor Público, los resultados de la información procesada. Equipo mediante el cual, en conjunto con el uso de la Red de Internet se puede ingresar a Programas o Aplicaciones remotas;

Hardware.- Conjunto de todas las partes tangibles de la Infraestructura. Sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos e incluye cables, gabinetes o cajas, de todo tipo y cualquier otro elemento físico involucrado. Es la contraparte complementaria del Software que es el soporte lógico en un elemento de Infraestructura;

Incidente.- Cualquier anomalía del funcionamiento normal o baja de desempeño de las aplicaciones o sistemas de información y violación al presente documento, que requieren atención de la Dirección;

Infraestructura.- Conjunto de bienes informáticos, cableado, equipos de cómputo, de radiocomunicación, conmutadores telefónicos, dispositivos móviles y otros equipos de naturaleza tecnológica, así como sus sistemas operativos, que funcionan como un sistema o como un conjunto de subsistemas;

Internet.- Conjunto de redes de equipos de cómputo y otros equipos físicamente unidos a través de medios alámbricos o inalámbricos que unen Redes o equipos en todo el mundo;

Lineamientos.- Conjunto de reglas y normas para la seguridad informática, que son de observancia particular y obligatoria establecidas en el presente documento.

Nodos.- Es un punto de conexión, ya sea de Redistribución (un ruteador o un switch) o de destino (Equipos de Cómputo), así como red de datos móviles;

Periféricos.- Dispositivos de entrada y de salida que se conectan a un Equipo de Cómputo. Por ejemplo: escáner, impresora, teclado, dispositivos móviles, entre otros;

Red.- Conjunto operacional de toda la Infraestructura de transmisión de datos propiedad del Organismo incluyendo equipos, configuraciones, cableados, enlaces propios o subcontratados y políticas de uso;

Servidor Público.- Los Trabajadores que prestan un servicio físico, intelectual, técnico o administrativo subordinado al Organismo Operador del Parque de la Solidaridad;

Servicios.- Son todas las aplicaciones que están soportadas en la infraestructura de tecnología propia y móvil, para agilizar y automatizar las actividades del Departamento con el servidor público;

Seguridad Informática.- Conjunto de controles y medidas necesarias cuya finalidad es resguardar y garantizar la protección, integridad, confidencialidad, acceso seguro y disponibilidad de la información institucional;

Sistema Operativo.- Programa o conjunto de programas computacionales que en un sistema informático (por ejemplo, un equipo de cómputo o dispositivo móvil) gestiona los recursos de Hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes;

Sistema de Información.- Cualquier programa computacional asociado a una o más base de datos, de uso específico para el Organismo que se encuentre en operación y que pueda haber sido desarrollado internamente por la Dirección, desarrollado y/o licenciado por uno o varios proveedores contratados para tal efecto; o bien, que esté bajo la administración de la Dirección. Los Sistemas de Información se encuentran instalados y configurados en la infraestructura de servidores pertenecientes al Data Center y sirve para soportar la operación interna general;

Soporte Técnico.- Conjunto de actividades preventivas y correctivas orientadas a mantener en operación los Servicios de Tecnología de la Información (TI) dentro de rangos aceptables de rendimiento, seguridad informática y que son desempeñadas por la Dirección;

Usuario/a.- Servidor Público que hace uso del Equipo de cómputo y red de datos propia y móvil;

Virus Informático.- Es un programa informático que se ejecuta en el Equipo de Cómputo sin previo aviso y que puede corromper el resto de los programas, directorios de datos e incluso el mismo Sistema Operativo, comprometiendo la seguridad e integridad de los datos generados por el Organismo Operador del Parque de la Solidaridad.

4. LINEAMIENTOS

DISPOSICIONES GENERALES

Artículo 2.- Los presentes Lineamientos serán aplicables a las áreas siempre y cuando reciban de parte de la Dirección acceso a la red y/o a uno o más sistemas de información, pudiendo ser de manera temporal o permanente; para tales efectos, tendrán que designar a un grupo de enlace que asuma las responsabilidades homólogas respecto al contenido de los presentes Lineamientos.

Artículo 3.- Las disposiciones sobre seguridad informática deberán seguir un proceso de actualización permanente en función del dinámico ambiente que rodea cada actividad sustantiva de las áreas, así como resultado de la innovación tecnológica social que debe ir a la par del avance de nuevas tecnologías que satisfagan la operación gubernamental.

Artículo 4.- La Dirección podrá dictar normas, reglamentos y protocolos a seguir donde se definan las medidas a tomar para proteger la seguridad informática, estas disposiciones podrán entrar en vigor en cualquier momento, con o sin previo aviso (llámese en casos de emergencia) a los servidores públicos o sus superiores jerárquicos. Estas disposiciones podrán incluir la intervención directa en los equipos de cómputo.

Artículo 5.- Los servidores públicos al conocer los presentes Lineamientos, deberán además observar y atender lo dispuesto en los siguientes ordenamientos:

I. Lineamientos para la Asignación y Uso de los Bienes Informáticos en el Organismo Operador de la Solidaridad;

II. Lineamientos para el Uso de los Sistemas de Información del Organismo Operador del Parque de la Solidaridad;

III. Lineamientos para el Uso Correcto del Servicio de Internet en el Organismo Operador del Parque de la Solidaridad.

Artículo 8.- La Dirección a través de las diferentes áreas del Organismo, deberán estar en estrecha coordinación para mantener el más alto nivel de seguridad informática que se pueda tener con los medios disponibles. Esta coordinación debe darse para planear y ejecutar la mejora de la seguridad informática contando con la intervención y apoyo de la Dirección.

Artículo 9.- La Dirección a través de las diferentes áreas del Organismo, implementará los mecanismos de control que eviten poner en riesgo la Seguridad Informática a causa de robo, fraude o sabotaje de la información.

Artículo 10.- Los medios de almacenamiento como memorias USB, discos DVD, etc., deberán ser destruidos antes de ser desechados. De la misma manera, los equipos de cómputo antes de darse de baja por el procedimiento respectivo, deberán ser formateados a bajo nivel.

Artículo 11.- La Dirección es la responsable de supervisar el cumplimiento de los presentes Lineamientos en las diferentes áreas del Organismo.

Artículo 12.- Los Servidores Públicos encargados de las diferentes áreas del Organismo, deberán informar de manera inmediata a la Dirección, sobre los incumplimientos detectados al respecto de los presentes Lineamientos.

Artículo 13.- La Dirección podrá apoyarse de las diferentes áreas para actividades específicas, al respecto de la seguridad informática de manera temporal o permanente.

5. OBLIGACIONES Y RESPONSABILIDADES DE LOS USUARIOS.

Artículo 14.- Los servidores públicos deberán encargarse de los siguientes procedimientos respecto a seguridad informática:

I. Utilizar la infraestructura de comunicaciones asociada a su equipo de cómputo, para acceder solamente a equipos locales o remotos a los que tenga autorización por parte de la Dirección;

II. Verificar que su equipo de cómputo tenga configurado el protector de pantalla con contraseña, con la finalidad de evitar el acceso no autorizado a su información en caso de retiro temporal;

III. Conectarse a la red cableada e inalámbrica únicamente con la autorización de los encargados de área;

IV. Resguardar en un lugar seguro los medios electrónicos en que tenga respaldada su información laboral relacionada con los servicios al Organismo;

V. Cambiar cada mes la contraseña asignada; siempre que los sistemas de información o aplicaciones lo permitan;

VI. Hacer uso exclusivo de las contraseñas asignadas por la Dirección, para lo cual, el servidor público deberá evitar compartirla o divulgarla;

VII. Los servidores públicos deberán contar con la autorización de la Dirección para conectarse a la Red de manera alámbrica o inalámbrica. La solicitud de la autorización deberá ser gestionada por un responsable del servicio;

VIII. Tener presente cuál es la información clasificada sobre la que tiene control en el desempeño de sus funciones. La información que se tenga almacenada en documentos electrónicos, se debe proteger con contraseña y podrá ser enviada o entregada únicamente a sus superiores. Cada envío de esta información reservada debe quedar registrado por escrito en documento impreso o en correo electrónico;

IX. Lo usuarios externos y sus empleadores deberán firmar un Convenio de Confidencialidad al respecto de la información a la que tendrán acceso por la naturaleza de las actividades que, de manera plenamente justificada, realicen dentro del Organismo.

Artículo 15.- Los servidores públicos deberán evitar realizar las siguientes acciones:

I. Conseguir o intentar conseguir los medios para acceder a sitios de Internet que no le son permitidos por la Dirección;

II. Acceder a sitios de Internet de contenido malicioso o de gestión de descargas;

III. Enviar cadenas por correo electrónico;

IV. Alterar o dañar los identificadores de los equipos de cómputo y/o sus periféricos;

V. Alterar la configuración de red que les fue asignada al momento de la instalación del equipo;

VI. Tener instalados programas de gestión de descarga los cuales al ejecutarse se constituyen amenazas a la seguridad informática pues facilitan una vía para accesos no autorizados a la Red, sistemas o información del Organismo;

VII. Tomar bebidas o ingerir alimentos en las áreas donde se encuentren instalados los equipos de cómputo y/o periféricos;

VIII. Instalar algún tipo de dispositivo (AP, Router, Switch) para replicar y comprometer la seguridad o estabilidad de la Red del Organismo, sin previa autorización o conocimiento de la Dirección.

IX. Habilitar o instalar servicios (DHCP, Servidores WWW, FTP) en alguna computadora para comprometer y/o replicar configuraciones de Red del Organismo, sin previa autorización o conocimiento de la Dirección.

X. El usuario no está habilitado para formatear o intervenir ningún equipo de cómputo, redes y telecomunicaciones del Organismo por su propia cuenta.

XI. Contravenir los presentes Lineamientos.

6. ATRIBUCIONES Y OBLIGACIONES DE LA DIRECCION

Artículo 16.- Son responsabilidades y obligaciones de la Dirección además lo dispuesto en los presentes Lineamientos, las siguientes:

I. Establecer las disposiciones aplicables acerca de seguridad informática para el Organismo;

II. Llevar a cabo auditorías sobre los equipos de cómputo que son responsabilidad de los servidores públicos respecto a la seguridad informática;

III. Verificar que todos los protocolos y servicios innecesarios sean deshabilitados en todos los equipos de cómputo;

IV. Asegurar que ningún elemento de infraestructura, aplicación o sistema de información, así como cuenta de usuarios carezcan de contraseña;

V. Mantener el control de la administración de los equipos de cómputo para permitir que sólo personal de las diferentes áreas del Organismo tengan acceso a los mismos;

VI. Realizar labores de investigación acerca de incidentes en los sistemas de información y elementos de infraestructura para determinar las causas de los mismos, y eventualmente, para deslindar responsabilidades;

VII. Instalar en los equipos de cómputo del Organismo, antivirus, sistemas de control de accesos, sistemas de monitoreo de código malicioso; así como éstas y otras definiciones sean actualizadas frecuentemente;

VIII. Administrar las contraseñas de administrador de todos los equipos de cómputo del Organismo;

IX. Modificar los procedimientos de acceso a los sistemas de información con la finalidad de mejorar la seguridad informática;

X. Asegurar que los nodos de cableado estructurado que no estén en uso, no estén habilitados; o si lo están, tengan habilitados en los puertos de switch el acceso por medio de listas de acceso o por dirección física de Red;

XI. Adquirir la infraestructura y/o sistemas para uso específico de seguridad informática más actual disponible dentro del presupuesto autorizado;

XII. Capacitar al menos una vez al año a los servidores públicos responsables de la seguridad informática en cuanto a infraestructura y antivirus, o cada que haya una adquisición de infraestructura que implique una actualización o mejora a la seguridad informática;

XIII. Facilitar a los servidores públicos responsables de la seguridad informática el acceso Permanente a información actualizada en esta materia.

7. DE LAS SANCIONES

Artículo 17.- La Dirección solicitará vía oficio a la Contraloría Estatal, para que en el ámbito de su competencia, inicie los procedimientos y aplique las sanciones por responsabilidad administrativa, relativas a los alcances de los presentes Lineamientos.

8. VIGENCIA

Articulo 18.- Los presentes Lineamientos entrarán en vigor a partir del veinticinco de octubre de dos mil diecisiete.