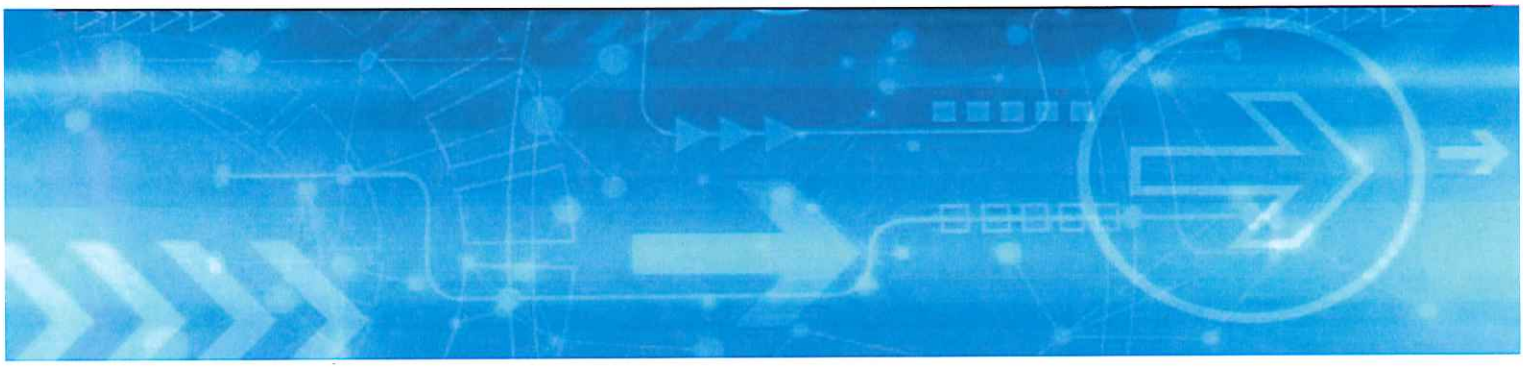


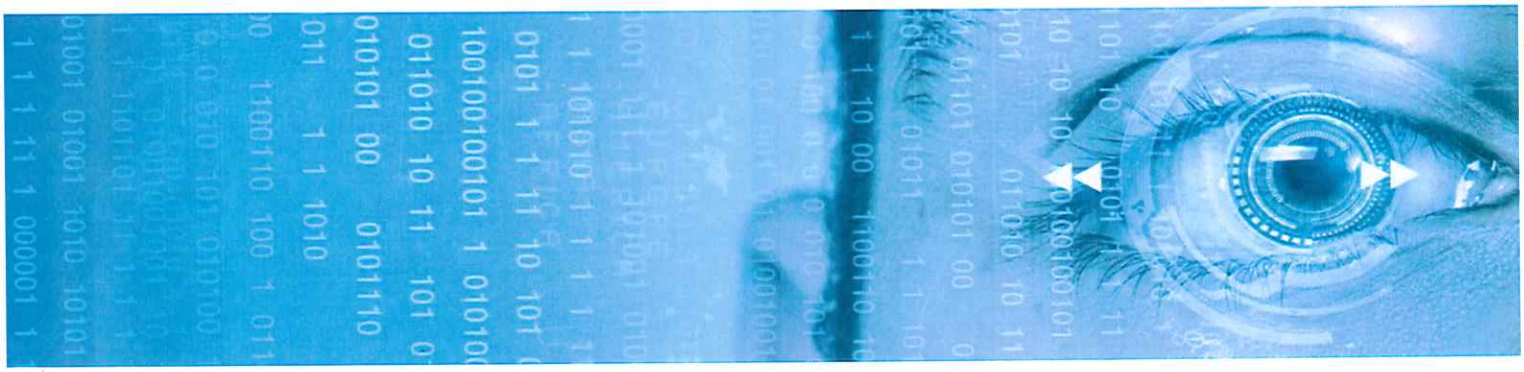
PLAN DE RECUPERACIÓN DE DESASTRES

Y

POLÍTICAS Y ESTÁNDARES

DE SEGURIDAD EN INFORMÁTICA

MUNICIPIO DE NEZAHUALCÓYOTL 2020



MANUAL
PLAN DE RECUPERACIÓN DE DESASTRES
POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
MUNICIPIO DE NEZAHUALCÓYOTL 2020

ÍNDICE

MANUAL
PLAN DE RECUPERACIÓN DE DESASTRES
POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
MUNICIPIO DE NEZAHUALCÓYOTL 2020

GLOSARIO

ADMINISTRACIÓN DE CRÍSIS: Proceso mediante el cual la organización administra el impacto del desastre, la cobertura adversa a medios de comunicación y mantenimiento continuo de información del avance del proceso de solución.

BISO: (sigla en inglés de basic input/output system; en español "sistema básico de entrada y salida") es un software que localiza y reconoce todos los dispositivos necesarios para cargar el sistema operativo en la memoria RAM.

COBIT: Objetivos de Control para Tecnología de Información y Tecnologías relacionadas, se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

COPIA DE SEGURIDAD (BACKUP): duplicación de información en medios de almacenamiento alternos con el fin de que sea un medio de contingencia para recuperarla en caso de desastre.

DESASTRE: Un evento que afecta a un servicio o sistema de manera tal que es requerido un esfuerzo importante para restablecer el nivel original de operación y desempeño.

RPD: Plan de Recuperación de Desastres, Proceso de recuperación que cubre los datos, el hardware y el software crítico, para que el Municipio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

TI: Tecnologías de la Información las relativas e implementadas por el H. Ayuntamiento de Nezahualcóyotl de obligación para los servidores públicos en lo referente.

Factores de Riesgo: es una condición real que se vive en todo el mundo, en el cual hay una exposición a la adversidad por una combinación de circunstancias del entorno donde hay posibilidad de pérdidas o debilidad de las tecnologías de la información. Los riesgos informáticos son exposiciones tales como atentados y amenazas a los sistemas de información, una amenaza se materializa, utilizando la vulnerabilidad existente de un gobierno de un activo o grupos de activos, lo que genera pérdidas de información y obstáculos para el cumplimiento de los objetivos de la Hacienda Municipal.

Calle Faisán N° 110 Col. Benito Juárez, C.P. 57000 Nezahualcóyotl Estado de México, Conmutador 57169070 Ext. 2302

Soporte Técnico: Las Áreas dependientes de cada una de las Direcciones que cuentan con Servidores de Almacenamiento de Información de la información que se procesa por la Administración Pública de Nezahualcóyotl, áreas responsables de la aplicación del Plan de Recuperación de Desastres de Tecnologías de la Información.
Historial: reporte del inicio y presente de un usuario, especificando su movimiento en el manejo de información, consultas en herramientas de Tecnología de la Información.

Noma ISO 20071: Norma internacional que se aplica específicamente a la gestión de tecnología de la información y en particular a la seguridad de la información. PC: Procesos Críticos de los activos de la información.

Plan de Contingencia: es un plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas. El plan de contingencia propone una serie de procedimientos cuando alguna de sus funciones usuales se ve perjudicada por un factor interno o externo.

Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

SAN: es una red dedicada al almacenamiento que está conectada a las redes de comunicación del Municipio.

Seguridad de la Información: Proceso continuo para salvaguardar la confidencialidad, integridad y disponibilidad de la información del Municipio, al igual que las características de la información como la autenticidad.

Usuario: servidor público que tiene acceso a las diversas tecnologías de la información que utiliza el Municipio y que se sujetara a los establecido por las áreas de Soporte Técnico en cuanto al Plan de Recuperación de Desastres de TI, y de las políticas que se establezcan.

Lineamientos de Tecnologías de la Información y Comunicación. Fuente obligacional de todos los servidores públicos del Municipio de Nezahualcóyotl en todo lo relacionado a las Tecnologías de la Información y Comunicación de Nezahualcóyotl.

CITIyC. Comité Interno de Tecnologías de la Información y Comunicación.

MANUAL
PLAN DE RECUPERACIÓN DE DESASTRES
POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
MUNICIPIO DE NEZAHUALCÓYOTL 2020

INTRODUCCIÓN

La necesidad de prestar servicios de calidad a través de sus trámites en el Municipio de Nezahualcóyotl ha generado que sus activos de información y los equipos informáticos sean recursos cada vez más importantes y vitales de nuestra forma de hacer gobierno y una ciudad para todos los habitantes de Nezahualcóyotl.

El buen uso y la disponibilidad que se tenga de todos los recursos informáticos desde equipos, estrategias y políticas, hacen que nuestras actividades sean más eficientes y eficaces; es por tal razón que tenemos el deber de preservarlos, utilizarlos y mejorarlos.

Lo que significa que se deben tomar las acciones, decisiones apropiadas en el Municipio de Nezahualcóyotl por parte de las Áreas de Soporte Técnico para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales. Por todo lo anterior, es necesario contar con un manual "Plan de Recuperación de Desastres Políticas y Estándares de Seguridad Informática" que norme las actividades relacionadas con los sistemas de información. Para lograr lo anterior, se pone a disposición el presente modelo de manual para que pueda ser adoptado por todas las Dependencias, haciendo las adecuaciones que corresponda al tamaño de la organización de su control interno y la madurez de las TIC´s y demás consideraciones relacionadas por las áreas de Soporte Técnico, las cuales deben darse a conocer a la Dirección de Administración del Municipio de Nezahualcóyotl, para ser presentadas al Comité de Tecnologías de la Información y Comunicación.

Calle Faisán N° 110 Col. Benito Juárez, C.P. 57000 Nezahualcóyotl Estado de México, Conmutador 57169070 Ext. 2302

MANUAL
PLAN DE RECUPERACIÓN DE DESASTRES
POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
MUNICIPIO DE NEZAHUALCÓYOTL 2020

OBJETIVO DEL MANUAL

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal, para que sea de su conocimiento y cumplimiento en el uso de los recursos informáticos asignados en situaciones de desastres.

GENERAL

Diseñar el plan de recuperación de desastres en el área de tecnologías de la información de la Fundación Neumológica Colombiana.

ESPECÍFICOS

Levantar la información de los factores de riesgo de los activos de la información.

Diseñar los tiempos de respaldo.
Diseñar el tiempo de recuperación o recovery time objective RTO.
Diseñar el punto de recuperación o recovery point objective RPO.
Diseñar diferentes escenarios en una posible recuperación de desastres.
Identificar las acciones del área de tecnologías de la información para mantener vigente el plan de recuperación de desastres.

Calle Faisán N° 110 Col. Benito Juárez, C.P. 57000 Nezahualcóyotl Estado de México, Conmutador 57169070 Ext. 2302

MANUAL
PLAN DE RECUPERACIÓN DE DESASTRES
POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
MUNICIPIO DE NEZAHUALCÓYOTL 2020

ALCANCE

El documento define las Políticas y Estándares de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos, lograr la Integridad, Confidencialidad y la Disponibilidad de la Información.

Integridad: que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento.

Confidencialidad: que la información sea accesible solo a las personas autorizadas.

Disponibilidad: que los usuarios autorizados tengan acceso a la información y los recursos cuando lo necesiten.

Sanciones por incumplimiento

El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa, haciéndose del conocimiento de tales hechos al Órgano de Control Interno para los efectos conducentes y/o de ser el caso por causa penal a las autoridades correspondientes, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

MANUAL
PLAN DE RECUPERACIÓN DE DESASTRES
POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
MUNICIPIO DE NEZAHUALCÓYOTL 2020

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política: Todo usuario de bienes y servicios informáticos se compromete a conducirse bajo los principios de confidencialidad de la información y del uso adecuado de los recursos informáticos, así como el estricto apego al Manual y estándares de informática, cumplir el Plan de Recuperación de Desastres y de las Políticas y Estándares de Seguridad Informática del presente manual.

1.1. Acuerdos de uso y confidencialidad. Todos los usuarios de bienes y servicios informáticos deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información, así como comprometerse a cumplir el Plan de Recuperación de Desastres y de las Políticas y Estándares de Seguridad Informática del presente manual.

1.2. Entrenamiento en Seguridad Informática. Todo empleado de nuevo ingreso deberá:

- Leer el Plan de Recuperación de Desastres y de las Políticas y Estándares de Seguridad Informática, el cual estará disponible en el portal de internet del Municipio de Nezahualcóyotl, donde se dan a conocer las obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.

- Firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de el Plan de Recuperación de Desastres y de las Políticas y Estándares de Seguridad Informática; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

1.3. Acuerdos de uso y confidencialidad a externos.

- Cada Dependencia por conducto del Director debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación del Plan de Recuperación de Desastres y de las Políticas y Estándares de Seguridad Informática, para el personal provisto por terceras partes, que realicen labores en o para la Dependencia o Entidad.

- Firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas y Estándares de Seguridad, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

- Todos los usuarios externos y personal de empresas externas deben estar autorizados por la Dependencia o Entidad, quien será responsable del control y vigilancia del uso adecuado de la información y los bienes y servicios informáticos.

MANUAL
PLAN DE RECUPERACIÓN DE DESASTRES
POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
MUNICIPIO DE NEZAHUALCÓYOTL 2020

2. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL.

Política: Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Entidad o Dependencia, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones de la Entidad o Dependencia.

La Entidad o Dependencia proveerá los mecanismos para su difusión y aplicación como fuente obligacional y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se cuente con la autorización de la dependencia y/o entidad y que estén acompañadas por un responsable del área de tecnologías de sistemas de información y comunicación del Municipio de Nezahualcóyotl.

Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido, salvo que la dependencia y/o entidad, den autorización en otros horarios por mayor seguridad y a efecto de no obstaculizar las funciones, servicios y atenciones a los ciudadanos del Municipio.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el responsable del área de tecnología de sistemas de información, a través de formatos de autorización de Entrada/Salida, de los cuales deberá en todo momento tener conocimiento el titular de la Dependencia.

MANUAL
PLAN DE RECUPERACIÓN DE DESASTRES
POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
MUNICIPIO DE NEZAHUALCÓYOTL 2020

2.1. Resguardo y protección de la información

2.1.1. Respaldo de la Información

La Dirección de Administración y aquellas que cuentan con su propia infraestructura de soporte a los sistemas de información y comunicaciones validarán la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades, la Dirección de Administración coordinara el respaldo y resguardo de la generación de copias de respaldo, la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información, informando y entregando los resguardo al responsable de la entidad.

Así mismo, La Dirección de Administración velará porque los medios de almacenamiento que contienen la información crítica sean resguardados en diferentes sitios. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

2.1.2. Copias de respaldo de la información

2.1.2.1. La Dirección de Administración, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

2.1.2.2. La Dirección Administración debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

2.1.2.3. La Dirección de Administración, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario en coordinación con aquellas áreas de soporte que cuenten con sus propios equipos de almacenamiento de información.

2.1.2.4. La Dirección de Administración y las Direcciones que en sus áreas de soporte técnico de tecnologías de la información y comunicación cuenten con fuentes de almacenamiento de la información (servidores), deben definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

2.1.2.5. Es responsabilidad de los usuarios de la plataforma tecnológica identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

2.1.2.6. El usuario deberá reportar de forma inmediata a la Dirección de Administración y/o Área de Soporte Técnico de la misma y de aquellas dependencias que cuenten con equipos de almacenamiento de la información, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

2.1.2.7. El usuario tiene la obligación de proteger los CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su resguardo, aun cuando no se utilicen y contengan información reservada o confidencial.

2.1.2.8. Es responsabilidad del usuario evitar en todo momento la fuga de la información que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

2.2. Controles de acceso físico de equipo

2.2.1. El resguardo de los equipos de cómputo deberá quedar bajo cada usuario al que le sea asignado y/o sea responsable de los equipos en cada una de las dependencias, así como del área de patrimonio municipal del Municipio que formará parte del control de inventario de bienes muebles Institucional, debiendo tener la Dirección de Administración el inventario de todos los equipos informáticos para su control que permita conocer siempre la ubicación física de los mismos.

2.2.2. Cualquier persona que tenga acceso a las instalaciones de la Entidad o Dependencia, deberá informar por escrito al titular de la dependencia del Ingreso de equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Dependencia o Entidad, el cual podrán retirar el mismo día, sin necesidad de trámite alguno, para este efecto el titular de la dependencia deberá información al titular de patrimonio municipal del ingreso de estos equipo para no ser susceptibles de ser inventariados por la Entidad.

2.2.3. En caso de que el equipo que no es propiedad de la Entidad o Dependencia permanezca dentro de la institución más de un día hábil, es necesario que el titular de la dependencia responsable de la oficina en el que trabaja el dueño del equipo, elabore y firme oficio de autorización de salida.

2.3. Controles de acceso físico a la Infraestructura de Comunicaciones

2.3.1. Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por personal de la Dirección de Administración y por aquellas Direcciones que en sus áreas de soporte técnico de tecnologías de la información y comunicación cuenten con fuentes de almacenamiento de la información (servidores); no obstante, los visitantes siempre deberán estar acompañados durante su visita a los centros de cómputo o los centros de cableado.

2.3.2. La Dirección de Administración y las Direcciones que en sus áreas de soporte técnico de tecnologías de la información y comunicación cuenten con fuentes de almacenamiento de la información (servidores) deben registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora que establezca la Dirección pajo su responsabilidad.

2.3.3. La Dirección de Administración y las Direcciones que en sus áreas de soporte técnico de tecnologías de la información y comunicación cuenten con fuentes de almacenamiento de la información (servidores) deberán descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

2.4. Infraestructura

2.4.1. Deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

2.4.2. Todo equipo de TI debe ser revisado, registrado y aprobado por la Dirección de Informática antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

2.4.3. La configuración de Routers, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Dirección de Administración y las Direcciones que en sus áreas de soporte técnico de tecnologías de la información y comunicación cuenten con fuentes de almacenamiento de la información (servidores).

2.4.4. La Dirección de Administración y las Direcciones con áreas de soporte técnico de tecnologías de la información y comunicación que cuenten con fuentes de almacenamiento de la información (servidores). Deben proveer las condiciones físicas y medioambientales necesarias para la protección y correcta operación de los recursos de la o las plataformas tecnológicas ubicadas en los centros de cómputo de almacenamiento; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

2.4.5. La Dirección de Administración debe velar porque los recursos de la plataforma tecnológica ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

2.4.6. La Dirección de Administración debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

2.5. Seguridad Perimetral

2.5.1. La seguridad perimetral es uno de los métodos posibles de protección de la Red del Municipio de Nezahualcóyotl, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

2.5.2. La Dirección de Administración deberá implementar soluciones lógicas y físicas que garanticen la protección de la información de la Entidad o Dependencia de posibles ataques internos o externos.

- Rechazar conexiones a servicios comprometidos.
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

2.5.3. Firewall

- La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, ya sean clientes o servidores.
- Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
- La Dirección de Administración y las Direcciones con sistemas de Tecnologías de la Información consistentes en fuentes almacenamiento (servidores) establecerá las reglas en el Firewall necesarias para bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- El firewall debe bloquear las "conexiones extrañas" y no dejarlas pasar para que no causen problemas.
- El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también el número de conexiones que se están produciendo, y en cuanto detecten que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
- Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

2.5.4. Sistemas de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés) es una aplicación usada para detectar accesos no autorizados a un computador/servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

- La Dirección de Administración implementará soluciones lógicas y físicas que impidan el acceso no autorizado a los equipos.

- Detección de ataques en el momento que están ocurriendo o poco después.

- Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.

- Análisis de comportamiento anormal, para revelar o descubrir una máquina comprometida o un usuario con su contraseña al descubierto o un sistema con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.

2.5.5. Conectividad Remota - Redes Privadas Virtuales (VPN)

La Dirección de Administración establecerá los requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Entidad y las dependencias; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

- La Dirección de Administración debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la Entidad y las dependencias.

- Los usuarios móviles y remotos de la Entidad o Dependencia podrán tener acceso a la red interna desde cualquier ubicación con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por la Dirección de Administración y por las Direcciones que por la importancia de la información utilicen tecnologías de la información en fuentes de almacenamiento (servidores).

- La Dirección de Administración y las Direcciones que cuentan con tecnologías de la Información consistentes en fuentes de almacenamiento (servidores), serán las encargadas de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.

- La Dirección de Administración y las Direcciones que cuentan con tecnologías de la Información consistentes en fuentes de almacenamiento (servidores), deben restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Entidad y deben acatar las condiciones de uso establecidas para dichas conexiones.

2.5.6. Conectividad a Internet

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los usuarios tienen las mismas responsabilidades en cuanto al uso de Internet.

- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.

- Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

2.5.7. Red Inalámbrica (WIFI)

La red inalámbrica es un servicio que permite conectarse a la red de Datos e Internet sin la necesidad de algún tipo de cableado.

Las condiciones de uso definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, IPad, celulares, etc.) con capacidad de conexión Wireless

2.5.7.1. Tecnología

- A pesar de que se usan amplificadores de señal, la cobertura queda sujeta a diversos factores, por lo que NO SE GARANTIZA en ninguna forma el acceso desde cualquier punto fuera de cobertura.

- La Dirección de Administración se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios.

- No se permiten la operación ni instalación de "puntos de acceso" (access points) conectados a la red cableada sin la debida autorización por parte la Dirección de Administración.

- No se permite configurar las tarjetas inalámbricas como "puntos de acceso" o la configuración de equipos como servidores adicionales.

- La Dirección de Administración, es la encargada de la administración, habilitación y/o bajas de usuarios en la red inalámbrica.

2.5.7.2. Identificación y activación

- Para hacer uso de la red inalámbrica, el solicitante necesariamente deberá ser empleado de la Entidad.

- Como primer paso para hacer uso de este servicio, se deben de registrar los usuarios que deseen la prestación del servicio mediante el control que establezca la Dirección de Administración, donde se señale el dispositivo que se conectará a la red inalámbrica.

- Se debe llevar un registro de las tarjetas inalámbricas de todos y cada uno de los dispositivos que se conecten a la red del Municipio.

- Para conectarse a la red inalámbrica se deberá emplear autenticación tipo WPA2 para lo cual los nombres de usuarios y contraseñas cambiarán periódicamente (de 6 a 12 meses) con la finalidad de proporcionarles seguridad en el acceso a los usuarios.

- La Dirección de Administración, determinará las medidas pertinentes de seguridad para usar las redes inalámbricas.

- La Dirección de Administración, se reservan el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de la red.

- No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.

- Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dados de alta, este necesariamente deberá comunicar a la Dirección de Administración para los efectos conducentes para su respectiva baja del equipo de la red inalámbrica.

2.5.7.3. Restricciones/prohibiciones de acceso a Internet

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

- El uso de programas para compartir archivos (Peer to Peer).

- El acceso a páginas con cualquier tipo de contenido explícito e indebido.

- El uso de sitios de videos en línea o en tiempo real.

- Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.

- Uso de JUEGOS "on line" en la red.

2.5.7.4. Excepciones

- Entre las medidas de seguridad se deberá configurar para restringir, algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso.

- En caso de eventos, cursos, talleres, conferencias, etc., se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos dos días hábiles.

- En el caso de estos eventos las restricciones para acceder podrán ser "anuladas" temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos dos días hábiles.

Acceso a Invitados:

- La red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura.

- La red inalámbrica es de tipo Portal Cautivo y se tendrá una lista de usuarios invitados con contraseñas que se actualizarán cada tres meses.

2.6. Servidores, Configuración e instalación

2.6.1. La Dirección de Administración y las Direcciones que cuenten con fuentes de almacenamiento en sus áreas respectivas (servidores) proveerán y supervisarán la operación de los servidores físicos y su rendimiento.

2.6.2 La Dirección de Administración y las Direcciones que cuenten con fuentes de almacenamiento en sus áreas respectivas (servidores) mantendrá actualizadas las configuraciones de servidores físicos, que componen el Centro de Datos del Municipio que podrán ser utilizados por las dependencias administrativas siempre y cuando las capacidades de los mismos lo permitan.

2.6.3. El servicio de aprovisionamiento de servidores será bajo el esquema de servidores virtuales.

2.6.4. En caso de que los requerimientos de desempeño y capacidad de los servidores requeridos superen las configuraciones existentes, la Dirección de Administración llevara a cabo los procesos necesarios para proveerles el servicio, tales como procesadores, memorias, discos duros y servicios de instalación de los mismos.

2.6.5. El aprovisionamiento de servidores a externos deberá ser respaldado vía oficio, con los requisitos de Hardware y Software, así como los requisitos de publicación de servicios vía Internet (IP pública, Dominio), y solicitud de acceso seguro vía VPN.

2.6.6. La Dirección de Administración, podrá limitar al acceso al equipo, en el cual se encuentran instaladas las aplicaciones y Bases de Datos, propias de las dependencias y/o unidades administrativas.

2.6.7. El administrador del servidor será responsable de la administración del mismo en su totalidad (sistema operativo, antivirus, aplicaciones instaladas y respaldos).

2.6.8. El administrador del servidor deberá acreditar la propiedad del licenciamiento de los sistemas a instalar en el servidor.

2.6.9. La dependencia y/o unidad administrativa responsable de la administración deberá implementar los métodos o acciones necesarias para garantizar la seguridad a nivel de información y Sistema Operativo incluyendo cualquier vulnerabilidad reportada, parches y actualizaciones necesarias para el óptimo funcionamiento del mismo.

2.6.10. La Dirección de Administración y las Direcciones que cuenten con fuentes de almacenamiento en sus áreas respectivas (servidores) en caso de que detecten alguna falla de seguridad, serán puestos fuera de producción (cuarentena) con el fin de evitar brecha de seguridad hacia los demás servidores del Centro de Datos Municipal.

2.6.11. Los servidores que proporcionen servicios a través de la red e Internet deberán: Funcionar las 24 horas del día los 365 días del año, recibir mantenimiento anual que incluya la revisión de su configuración. Ser monitoreados.

2.6.12. La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo: Diariamente, información crítica.

2.6.13. Los servicios hacia Internet sólo podrán proveerse a los servidores autorizados por la Dirección de Administración.

2.7. Seguridad en Centro de Datos (Data Center)

El Centro de Datos de cada una de las Direcciones que cuentan con fuentes de almacenamiento de la información (servidores) son áreas restringidas, por lo que sólo el personal autorizado por las citadas Direcciones responsables de los servidores de Informática puede acceder a ellos.

2.7.1. Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la Dirección de Administración. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito de la Dirección de Administración.

El Data Center deberá:

Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por la Dirección de Administración y de las Direcciones que cuenten con sus propios servidores.

Recibir limpieza, que permita mantenerse libre de polvo.

Estar libre de contactos e instalaciones eléctricas en mal estado.

Controles de humedad y temperatura. Mantener la temperatura a 21 grados centígrados.

Asignar un técnico para que realice un control diario de temperatura y aires acondicionados y llevar un registro de estos controles.

Sistemas de Detección y extinción de incendio.

Los sistemas contra incendios deberán recibir mantenimiento anual con el fin de determinar la efectividad del mismo.

2.8. Protección y ubicación de los activos tecnológicos

Los recursos tecnológicos, deben ser utilizados de forma ética y en cumplimiento de los Lineamientos del Comité Interno de Tecnologías de la Información y Comunicación del Municipio de Nezahualcóyotl vigentes, con el fin de evitar daños o pérdidas sobre la operación.

2.8.1. Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un usuario, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

2.8.2. Los recursos tecnológicos provistos a funcionarios y personal suministrado por terceras partes son proporcionados con el único fin de llevar a cabo las labores asignadas; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

2.8.3. El personal no debe utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

2.8.4. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Dirección de Administración, debiéndose solicitar a la misma en caso de requerir este servicio.

2.8.5. La Dirección de Administración y las Direcciones en general serán las encargadas de generar las responsivas de resguardo de los usuarios de equipos de cómputo responsables de los archivos, bases de datos, padrones que se le asignen y de conservarlos en la ubicación autorizada por la Direcciones respectivas.

2.8.6. El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones asignadas al usuario.

2.8.7. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

2.8.8. Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.

2.8.9. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

2.8.10. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.

2.8.11. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

2.8.12. El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

2.8.13. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser debidamente autorizados por el titular del área que corresponda.

2.8.14. Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

2.8.15. La Dirección de Administración debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

2.8.16. La Dirección de Administración es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores y proporcionar, de así considerarlo, respaldo a las Dirección que requieran dicha información.

2.9. Uso de Dispositivos Móviles

2.9.1. La Dirección de Administración proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos.

2.9.2. La Dirección de Administración debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la Dependencia o Entidad.

2.9.3. Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

2.9.4. Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software que se les instale provisto con ellos al momento de su entrega.

2.9.5. Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

2.9.6. Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

2.9.7. Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

2.9.8. Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

2.10. Mantenimiento de Activos Informáticos e Infraestructura

El personal autorizado para el mantenimiento se encargará de proporcionar oportuna y eficientemente, los servicios que requieren las Dependencia usuarias en la Entidad en materia de mantenimiento preventivo y correctivo a los activos informáticos y a la infraestructura.

2.10.1. Únicamente el personal autorizado por la Dirección de Administración podrá llevar a cabo el mantenimiento preventivo y/o correctivo al equipo informático e infraestructura, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso.

2.10.2. El período para llevar a cabo el mantenimiento preventivo será determinado por la Dirección de Administración.

2.10.3. Queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no sea propiedad de la Entidad.

2.10.4. En caso de ser necesario un mantenimiento correctivo de cualquier equipo de cómputo, deberá de solicitarse a través de la Dirección de Administración.

2.10.5. El tiempo de reparación dependerá del nivel de daño o tipo de problema presentado en el equipo y en caso de ser necesario, se enviará a reparación especializada por parte de la Dirección de Administración.

2.10.6. Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación, solicitando la asesoría del personal de la Dirección de Administración por conducto de su área de soporte técnico.

2.11. Pérdida o transferencia de equipo

2.11.1. El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo con la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

2.11.2. El resguardo para las laptops tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

2.11.3. El usuario deberá dar aviso de inmediato a la Dirección de Administración, Consejería Jurídica, Secretaria del H. Ayuntamiento y Contraloría Municipal de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo, realizando lo conducente de acuerdo a la normatividad vigente.

2.12. Uso de periféricos y medios de almacenamiento

El uso de periféricos y medios de almacenamiento en los recursos de las plataformas tecnológicas de la Entidad será implementado por la Dirección de Administración y por aquellas Direcciones que prestan servicios de atención a la ciudadanía respectivamente, considerando sus necesidades de uso, estableciendo para ellos lineamientos o condiciones para dichos fines.

2.12.1. La Dirección de Administración y aquellas Direcciones que prestan servicios de atención a la ciudadanía respectivamente deben implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica, de acuerdo con los lineamientos y condiciones establecidas.

2.12.2. La Dirección de Administración y aquellas Direcciones que prestan servicios de atención a la ciudadanía respectivamente, deben aplicar lineamientos para la disposición segura de los medios de almacenamiento, ya sea cuando son dados de baja o reasignados a un nuevo usuario.

2.12.3. El personal de las Dependencias y personal provisto por terceras partes deben apegarse a las condiciones de uso de los periféricos y medios de almacenamiento establecidos por las Direcciones respectivas.

2.12.4. El personal de la Dependencias o personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por las Direcciones Respectivas.

2.12.5. El personal de la Dependencia es responsable por la custodia de los medios de almacenamiento asignados.

2.12.6. El personal de la Dependencia y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica.

2.13. Uso de dispositivos especiales

2.13.1. El uso de los grabadores de discos compactos es exclusivo para respaldos de información que, por su volumen, así lo justifiquen.

2.13.2. La asignación de este tipo de equipo será previa justificación por escrito, autorización y/o suministro de la Dirección de Administración.

2.13.3. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

2.13.4. Los módems internos deberán existir solo en las computadoras portátiles y no se deberán utilizar dentro de las instalaciones de la institución para conectarse a ningún servicio de información externo, excepto cuando lo autorice la Dirección de Administración.

2.14. Daño del equipo.

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso se determinará la causa de dicha descompostura.