POLITICA DE SEGURIDAD DIGITAL		

POLITICA DE SEGURIDAD DIGITAL

TABLA DE CONTENIDO

1. INTRODUCCION

Las políticas de seguridad definidas en el presente documento están dirigidas a los servidores públicos de la Alcaldía de Madrid Cundinamarca, las cuales serán de obligatorio cumplimiento, a fin de proteger la información y otros activos informáticos de amenazas y vulnerabilidades y garantizar la integridad, confidencialidad y disponibilidad de la información.

Con la definición de las políticas y estándares de seguridad informática, se busca establecer en el interior de la Alcaldía Municipal de Madrid una cultura de calidad operando en una forma confiable.

2. DEFINICION DE SEGURIDAD DE LA INFORMACION

La información es considerada un activo esencial en las actividades de la organización, es por ello que se deben establecer estrategias que permitan el control y administración de los datos, así como el uso adecuado de los recursos informáticos tanto de Hardware como de Software. De ahí la importancia de definir y dar a conocer políticas y procedimientos de seguridad que permitan proteger los Sistemas de Información de las amenazas a las que se encuentra expuesto por el uso de tecnologías de la información y asegurar la continuidad de los procesos y el logro de los objetivos institucionales.

3. OBJETIVO

Las políticas de seguridad informática, comprende un conjunto de reglas a ser aplicadas a todas las actividades relacionadas con los sistemas de información que soportan los procesos críticos de la Entidad, con el objeto de:

- Garantizar la integridad, confidencialidad y disponibilidad de la información
- Proteger los recursos tecnológicos.
- Minimizar el riesgo en los procesos críticos de la Entidad
- Cumplir con los principios de la función Administrativa
- Apoyar la innovación tecnológica
- Implementar el Sistema de Gestión de la Seguridad Informática SGSI
- Fortalecer la cultura de autocontrol de la información
- Garantizar la continuidad de los procesos frente a los incidentes.

4. ALCANCE

Las políticas de seguridad informática y controles serán de obligatorio cumplimiento para todos los servidores públicos de planta, contratistas y terceros que hagan uso de los activos de información de la Alcaldía de Madrid.

El incumplimiento al presente documento, podrá presumirse como causa de responsabilidad administrativa y/o disciplinaria, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Las excepciones al cumplimiento de las políticas de seguridad informática serán autorizadas única y exclusivamente por la Dirección de Sistemas de Información, cuando se considere que su impacto es negativo para la continuidad de los procesos o logro de los objetivos institucionales, y deberán ser documentadas formalmente.

Las políticas de seguridad informática serán objeto de evaluación semestral, aplicando mecanismos de autocontrol y autoevaluación, para garantizar el mejoramiento continuo.

5. TERMINOLOGIA Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la Organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la Organización.

Administrador de equipo: Persona responsable de configurar, administrar controladores de dominio o equipos locales, sus cuentas de usuario, asignar contraseñas, permisos y ayudar a los usuarios a solucionar problemas de red.

Administrador de Bases de Datos (DBA): Persona responsable de los aspectos ambientales de una base de datos.

Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Backups: Es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Base de Datos: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]: Característica o propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control de Acceso: Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Hardware: Se refiere a las características técnicas y físicas de las computadoras.

Integridad: Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.

IP: Etiqueta numérica que identifica de manera lógica y jerárquica a una interfaz (Elemento de comunicación/conexión) de un dispositivo dentro de una red que utilice el Protocolo IP.

Plan de Contingencia: Es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.

Redes: Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de onda.

Servidores: Computador que responde peticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistemas de Información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Software: Programas y documentación de respaldo que permite y facilita el uso del PC. El software controla la operación del hardware.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

6. POLITICAS Y CONTROLES

POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACION

La Alcaldía de Madrid ha establecido las siguientes políticas de seguridad, las cuales representan el interés de la Administración de proteger los Activos de Información.

Las políticas de seguridad de la información estarán contenidas en un documento que surtirá el trámite de aprobación de conformidad con el procedimiento de control de documentos y será publicado y comunicado a todos los servidores públicos por la Dirección de Sistemas de Información.

Las políticas de seguridad de información serán objeto de evaluación semestral, aplicando mecanismos de autocontrol y autoevaluación, para garantizar el mejoramiento continuo.

Política y Controles de Organización Interna

El nivel Directivo de la Alcaldía de Madrid, se compromete a apoyar activamente la seguridad de la información, el cual se verá reflejado en:

- Creación de un comité de seguridad digital interdisciplinario conformado por el Secretario de Planeación, Director de Sistemas de Información, Secretario Jurídico, Secretario General y Desarrollo Institucional, Profesional Universitario responsable del archivo, quienes serán los encargados de tratar los temas concernientes a la seguridad de la información, formulando su propio reglamento, en el cual establecerán responsabilidades, funciones y periodicidad de las reuniones.

Actuarán como invitados permanentes los Administradores de los diferentes sistemas de información.

- Asignación de un responsable de la seguridad de la información (Oficial de seguridad)
- Aprobación del documento de políticas de seguridad de la información.
- Velar por el cumplimiento de las políticas de seguridad de la información.
- Asignación de responsabilidades asociadas al tema de la seguridad de la información.

Políticas de Autorización para los Servicios de Procesamiento de Información

Objetivo: minimizar los riesgos de falla en los sistemas, velar por la utilización adecuada de los recursos y garantizar que estos contribuyan con el cumplimiento de los objetivos institucionales**.**

Política: La Dirección de Sistemas de Información será la responsable de definir y establecer los estándares y procedimientos para el desarrollo, mantenimiento y adquisición de sistemas de información, incluyendo la custodia del código fuente, ambientes de desarrollo, pruebas y producción, y de toda la infraestructura tecnológica relacionada, de conformidad con las mejores prácticas y reglas internacionales de seguridad informática.

Controles de Automatización de Procesos

Desarrollo de Aplicativos

Cualquier solicitud para el Desarrollo de aplicativos nuevos debe tener un proyecto de viabilidad el cual deberá estar debidamente sustentado, una vez sea aprobado por la Dirección de Sistemas de Información se ordena iniciar con las fases del ciclo de vida del sistema de información.

Control de Cambios

Al momento que una dependencia requiera alguna modificación, estructural o no, sobre el software aplicativo y si el proceso involucra más de una Dependencia, es necesario que la solicitud de modificación esté autorizada mediante escrito por los secretarios de despacho y personas responsables de la ejecución del proceso, de conformidad con el procedimiento establecido.

Control de Versiones

El Director de Sistemas de Información será el responsable de gestionar el control de las distintas versiones de desarrollo de un software, de tal forma que se garantice la confidencialidad, integridad y actualización de los documentos.

Publicación de Aplicativos

Para la publicación y puesta en marcha de aplicativos nuevos estos deben estar correctamente diseñados, evaluados de forma minuciosa para evitar la redundancia en las salidas de información, supervisados y autorizados por el Director de Sistemas de Información y el responsable del proceso.

Política de Confidencialidad de la Información

Todos los servidores públicos que manipulen información en cumplimiento de sus funciones, y terceros tales como proveedores de redes y servicios de telecomunicaciones, personal de entes de control entre otros, deben aceptar acuerdos de uso y manejo de la información reservada o confidencial definida por la Entidad, donde se comprometen a no revelar, modificar, dañar, eliminar o usar inapropiadamente la información confidencial a la que tengan acceso, so pena de las investigaciones penales y disciplinarias a las que haya lugar.

Controles

La Entidad identificará la información considerada clasificada o reservada, índice que deberá ser divulgada de conformidad con la normatividad vigente.

La Entidad establecerá controles para el intercambio de información con terceros para asegurar la reserva e integridad de la misma y que se respeten los derechos de autor.

La información clasificada reservada confidencial solo se debe transmitir por medios seguros.

Política de Seguridad de acuerdos con terceros

Los acuerdos con terceras partes que impliquen acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de la información de la Alcaldía de Madrid o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los controles pertinentes a fin de minimizar los riesgos y de mantener la seguridad de la información y de los servicios de procesamiento.

Controles

La Entidad identificará los riesgos para la información y servicios de procesamiento de información que involucran a terceros e implementará los controles adecuados antes de autorizar el acceso.

La Entidad considerará todos los requisitos de seguridad de la información identificados, antes de dar acceso a los activos de información a partes externas.

GESTION DE ACTIVOS

Política de Generación y Restauración Copias de Seguridad
(Ver el procedimiento de backup PPD-P-021)

En la Alcaldía de Madrid todo activo de información que sea de interés para un proceso operativo o de misión crítica de la Entidad, deberá ser respaldado con copias de seguridad, en la frecuencia que establezca la Dirección de Sistemas de Información y de conformidad con el procedimiento de backup PPD-P-021.

Controles:

En ningún caso las copias de seguridad serán almacenadas en el mismo equipo donde se encuentra la información.

Los medios de almacenamiento de las copias de seguridad estarán ubicados en sitios seguros para impedir el acceso a la información a personal no autorizado.

Los servidores públicos efectuaran copias de seguridad cuando los equipos de cómputo sean enviados a mantenimiento, previniendo así la perdida de información.

Los Administradores de las bases de datos realizaran pruebas de restauración de los backups con la periodicidad establecida en el procedimiento de backup, para garantizar que las copias son leídas y restauradas correctamente.

La Dirección de Sistemas de Información llevará un registro de las copias de respaldo recepcionadas y determinará conjunto con las Dependencias el esquema de copias de seguridad a implementar, de conformidad con el tipo de información y uso de la misma en los procesos operativos o de misión crítica para la Entidad.

La Dirección de Sistemas de Información conservará las copias de seguridad en un lugar externo a los del origen de la información, el cual debe contar con las medidas de protección y seguridad física adecuadas.

Política de Archivo de Documentos y Retención de Datos

Política: En la Alcaldía de Madrid, el archivo de los documentos producidos en la ejecución de los procesos, se efectuará de conformidad con las Tablas de Retención Documental aprobadas, el procedimiento de control de registros en lo relacionado con el archivo y retención de documentos, y lo establecido por el Archivo General de la Nación.

Control: Mediante el uso de la plataforma WINISIF –Módulo de Gestión Documental se conformarán expedientes virtuales de conformidad con las Tablas de Retención Documental aprobadas.

Políticas para el Manejo de los Datos Uso Compartido

Política: La Dirección de Sistemas de Información autoriza el uso compartido de carpetas que se crea en nuestro servidor ZEUS, pero no es responsable por las acciones y el acceso a la carpeta de la información compartida, los responsables serán los funcionarios de cada dependencia que tengan acceso a la misma.

Controles

La Dirección de Sistemas de Información autoriza la carpeta compartida delimitando a los usuarios que realmente la necesitan y controlar el tiempo en el cual estará expuesta.

La Dirección de Sistemas de Información autoriza la carpeta compartida y debe asegurarse que el usuario autorizado cuente con el antivirus institucional (Eset Nod 32).

Antivirus

Política: Todos los equipos de la entidad deben tener instalado, en funcionamiento, actualizado y debidamente licenciado el antivirus Eset Nod 32, el cual será suministrado por la Dirección de Sistemas de Información.

Controles:

El antivirus se debe instalar con opción de actualización automática.

Está prohibido que los usuarios desinstalen el antivirus de su equipo, modifiquen o eliminen las configuraciones de seguridad que previenen la propagación de virus, ya que esta acción puede ocasionar riesgo total de contaminación de virus.

Los usuarios deben asegurarse que todos los medios de almacenamiento tanto internos como externos están libres de virus o software malicioso, mediante la ejecución del software antivirus autorizado.

Los usuarios que tengan conocimiento del alojamiento de un virus en su PC deben comunicar de manera inmediata a la Dirección de Sistemas de Información para que le brinden el soporte técnico de erradicación del virus.

Todos los archivos anexos a los mensajes recibidos en el correo institucional, estarán sujetos al análisis del antivirus, y el destinatario final recibirá solo los que hayan sido exitosos.

Bases de Datos

Política: El Administrador de bases de datos, no podrá manipular directamente los datos, salvo en circunstancias en las cuales los aplicativos no lo permitan, y solo lo realizará cuando medie autorización escrita del líder del proceso propietario de la información, y con el debido soporte que requiera de la actualización respectiva.

Controles:

Se deben programar todas las tareas de afinamiento de las bases de datos y los sistemas de información de manera periódica, de acuerdo con la cantidad de solicitudes o quejas de los usuarios respecto de la disponibilidad de las aplicaciones.

El acceso a las bases de datos de los sistemas se realizará de conformidad con las políticas de acceso.

Las pistas de auditoría deben permitir monitorear las conexiones a las bases de datos, las modificaciones al modelo de datos y las modificaciones a los datos, de manera directa o por medio de aplicativos.

Los soportes documentales de las modificaciones a los datos de manera directa por los usuarios Administradores, deben conservarse de conformidad con las TRD aprobadas.

Medios de Almacenamiento Removibles

Política: Los servidores públicos que contengan información confidencial de propiedad de la Entidad en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

Controles:

Los medios de almacenamiento con información crítica deberán ser manipulados y enviados al tercero única y exclusivamente por la persona asignada por la Dirección de Sistemas para hacer respaldos y salvaguardar información.

Todo medio de almacenamiento con copias de seguridad debe ser marcado de acuerdo a la información que almacena, detallando su contenido.

Toda copia de respaldo que se encuentre en medios de almacenamiento removible deberá ser guardada bien sea en caja bajo llave o en un lugar seguro, al cual solo tendrá acceso el responsable de esta.

No está autorizado el uso de los dispositivos de almacenamiento externos removibles que contenga información de la Entidad, en lugares de acceso público como cibercafés o en equipos que no garanticen la confiabilidad e integridad de la información.

La información de la Entidad clasificada como confidencial que sea transportada en medios de almacenamiento removible, debe ser protegida mediante cifrado o contraseñas, para garantizar que no pueda ser vista por terceros en caso de robo o extravío.

Los equipos servidores tendrán deshabilitada la reproducción automática de dispositivos externos de almacenamiento removibles.

Modificación de Estructuras de Directorios y Carpetas

Política: Los Administradores de los sistemas de información son los únicos autorizados para manipular las estructuras de los directorios y carpetas, de acuerdo con sus especificaciones.

Encadenado de Información entre Documentos y Archivos

Política: Todo documento considerado confidencial debe ser auto contenido y no depender de la disponibilidad e integridad de fuentes externas de datos.

Nombres de Carpetas y Archivos

Política: La identificación de las carpetas y archivos debe ser lógico y de fácil identificación, y debe cumplir con los estándares de nombramiento establecidos por la Dirección de Sistemas de Información.

Protección de Documentos para su Distribución

Política: Los documentos que son distribuidos o compartidos con terceros, tendrán con marca de agua la clasificación de la información contenida, y su copia magnética se realizará en formato PDF de solo lectura, para impedir la modificación o eliminación accidental o intencional de los datos, y la pérdida de la confidencialidad inadvertida.

Control: Cada funcionario se hace responsable de la administración y distribución de la información existente en su equipo de cómputo, generando las respectivas copias de seguridad y en caso de ser necesario se entregará copia de esta a la Dirección de Sistemas para salvaguardar la información.

Uso del correo electrónico (ver política ppd-m-002)

Política: El Correo Electrónico es proporcionado por la Dirección de Sistemas de Información con el objeto de apoyar las funciones de comunicación a los funcionarios de la Alcaldía de Madrid Cundinamarca. Los Términos de Uso que se describen a continuación PPD-M-002 constituyen el acuerdo entre la Entidad y cualquier Usuario del Correo Electrónico, por lo tanto, es responsabilidad del usuario leerlos previo al uso del correo, de tal manera que conozca y acepte plenamente las condiciones de uso.

Controles:

Administración del Correo Institucional: El uso del correo institucional es de carácter institucional, siendo responsabilidad la administración del mismo de un funcionario de la Dirección de Sistemas.

El tamaño del buzón, de los archivos enviados y del contenido del correo será definido por la Dirección de Informática.

Cambio de Contraseñas a Correos Institucionales: En el mismo instante en que el Grupo de Sistemas de Información cree y dé a conocer de la cuenta de correo Institucional designada para cada Dependencia la persona encargada ingresara por primera vez y este automáticamente le solicitara el cambio de contraseña. La confidencialidad y el uso del usuario y contraseña será responsabilidad de la persona a quien se le asigne.

Envíos y Transferencias en Correos Institucionales: Todo correo institucional debe ser descargado periódicamente de la bandeja de entrada para así liberar y dar capacidad al servidor, garantizando la seguridad de la información, por cuanto la información institucional contenida en el buzón es propiedad de la Alcaldía.

Copias de seguridad de los correos institucionales: Mensualmente el Grupo de Sistemas de Información o persona encargada debe realizar Backups de todas las cuentas a través del servidor de correo, dicha persona no debe tener acceso a las claves propias de cada cuenta.

Recepción e Intercambio de información: El intercambio de información entre la Entidad y terceros a través de correos electrónicos, se hará única y exclusivamente por medio de los correos institucionales, y en ningún caso por medio de correos personales.

La información contenida en archivos generados en suite ofimáticas, será enviada en formatos no editables utilizando el software que brinde la Dirección de Sistemas de Información.

El usuario responsable del correo institucional debe evitar abrir los adjuntos de correos de origen desconocido o que contengan palabras en Ingles a fin de evitar los virus, a menos que haya sido analizado previamente por el antivirus autorizado.

El correo institucional será de uso exclusivo para fines propios de la Entidad y en su uso se dará aplicación al código de ética; En consecuencia, es prohibido utilizar el correo institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

Los usuarios del correo institucional deben evitar enviar respuestas a todos los destinatarios del correo inicial, salvo en los casos que sea absolutamente necesario, sobre todo en los casos en los cuales el correo original fue enviado de manera masiva.

Exoneración de responsabilidades: La Dirección de Sistemas de Información definirá el texto de exoneración de responsabilidad que se debe incluir en los correos electrónicos, para proteger a la entidad de los contenidos de los correos electrónicos.

Acceso a internet, intranet y portal web (ver procedimiento ppd-p-012)

Objetivo: Proveer la información necesaria a los usuarios sobre las políticas y controles a aplicar para hacer uso de los recursos de Internet, Intranet y portal Web del Municipio de Madrid.

Política: En la Alcaldía de Madrid el acceso a Internet e Intranet es permitido a todos los servidores públicos para facilitar el desarrollo de los procesos propios de la Entidad, no obstante, están obligados a cumplir con los controles de acceso y uso implementados por la Dirección de Sistemas de Información.

Controles:

Creación de Perfiles

Se crean cuatro (4) perfiles de usuario con los cuales se pretende controlar el acceso a internet, descongestionar el ancho de banda y garantizar la seguridad de la información.

Perfil No 1 Administrador: Corresponde a usuarios con funciones de Administradores de los sistemas de Información, con permisos para descargar archivos ejecutables

Perfil No 2. Comunicador: Usuarios de la oficina de prensa, cultura y otros que para el cumplimiento de sus funciones requieran acceso a redes sociales, reproducción de videos, emisoras en línea, sin descarga de archivos ejecutables

Perfil No 3 Comunicación General: Usuarios con acceso a redes sociales, reproducción de videos.

Perfil No 4 General: Corresponde a usuarios con acceso a internet y restricción a redes sociales, reproducción de videos.

Asignación IP: El Grupo de Informática debe tener en un archivo el registro de asignación y control del direccionamiento IP de cada uno de los equipos conectados que forman parte de la red con acceso a internet de la Alcaldía de Madrid, dicho debe contener la siguiente información:

1. Fecha en que es asignada la IP
2. Nombre del funcionario
3. Placa del equipo
4. Dependencia
5. Número de IP
6. Firma de la persona a la que se le asignó la IP

Finalidad del uso de internet: los canales de acceso a internet de la Entidad no podrán ser usados para fines diferentes a los requeridos en el desarrollo de las actividades propias de los cargos. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Alcaldía o de las personas.

La Alcaldía de Madrid se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad.

El uso de Internet para la revisión de correo electrónico personal, en cumplimiento de actividades propias de la Entidad, está autorizado siempre y cuando se observen los mismos lineamientos estipulados para la utilización del servicio de correo institucional.

Uso de la Intranet

Las cuentas de acceso a Intranet serán administradas por la Dirección de Sistemas de Información y serán creadas para personal de planta.

El personal de contrato por prestación de servicios de apoyo a la Gestión y Profesional podrán ser usuarios de la Intranet con previa autorización del director o secretario de la Dependencia en la cual se Desempeña.

Para el uso de Intranet se deben observar las mismas normas de comportamiento definidas para el uso de internet.

Publicación Portal Web

Administración de los Contenidos Institucionales de las Páginas: La administración de los contenidos de las páginas institucionales estará a cargo del grupo o comité designado para eso, quienes serán los encargados de verificar los contenidos que pueden o deben ser publicados. Todo contenido deberá respetar la ley de derechos de autor.

Ningún contenido del portal WEB se puede copiar con fines comerciales, ni se puede copiar y utilizar en otros sitios WEB.

Editores de los Contenidos Institucionales de las Páginas: Cuando por omisión un editor del portal web deje sus contraseñas o las revele, se hará responsable de todo lo realizado con este usuario.

Restricción para descarga de Software: La actividad de descarga de software estará a cargo de la persona o grupo de personas definido por el grupo de informática, por lo tanto, los usuarios de internet no están autorizados para descargar software, música, juegos, películas, protectores de pantalla, etc. Así como efectuar pagos, compras de bienes o servicios a través de los canales de acceso a internet de la Alcaldía a título personal o de la Entidad, salvo cuando medie autorización.

Los Usuarios de Internet no están autorizados para descargar herramientas que comprometan la seguridad con actos como monitoreo de datos, sondeo, copias, prueba de firewalls o hacking entre otros.

<u>Configuración y administración de las redes</u>

Política: La Dirección de Sistemas de Información contará con personal capacitado, responsable de la configuración y administración de las redes de tal forma que se garantice el control de acceso y la restricción de privilegios, dando aplicación al protocolo que se establezca para tal fin.

Los usuarios de la Red de la Alcaldía de Madrid no deben establecer redes de área local, conexión remota a redes internas o externas, o transferir archivos a través del servidor FTP, utilizando la red de la Entidad sin autorización previa de la Dirección de Sistemas de Información.

Controles

El acceso ala Red Inalámbrica de la Alcaldía de Madrid a través de equipos de telefonía móvil será restringido por la Dirección de Sistemas de Información, a fin de minimizar los riesgos y mejorar la velocidad en la navegación desde equipos portátiles, siendo este el fin principal de este tipo de tecnología.

La Dirección de Sistemas de Información es la responsable de la configuración apropiada e instalación de mecanismos de detección de intrusos y sistemas de protección del Hardware (firewalls), Software base, aplicativos, redes y sistemas de comunicación, a fin de evitar la intrusión y los ataques físicos.

<u>Adquisición y mantenimiento de software y hardware (ver el procedimiento pdd-p-018)</u>

Política: Toda adquisición de recurso tecnológico en la Alcaldía de Madrid, deberá contar con la revisión y aprobación previa de los requerimientos técnicos mínimos definidos, por parte de la Dirección de Sistemas de Información.

El software registrado con Derechos de Autor no se podrá copiar sin previa autorización del propietario.

Política: Todo proceso de cambio de Software deberá contar con un plan de contingencia, de tal forma que se garantice la continuidad de los procesos, la salvaguarda e integridad de la información.

Controles:

Adquisición de Equipos de Cómputo: La Dirección de Sistemas de Información verificará las características y el estado de todos los equipos digitales y análogos que ingresan a la Alcaldía de Madrid, previo al ingreso a almacén.

Todos los dispositivos adquiridos deben contar con la garantía de fábrica y debe acreditarse con documento equivalente a certificación o documento expedido por la casa fabricante de cada dispositivo, la cual debe tener el tiempo de garantía, tipo de garantía y tipo de cubrimiento.

Los equipos que hayan sido importados deben contar con el certificado de manifiesto de aduana.

La CPU y los periféricos como son monitor, mouse y teclado que adquiera la Entidad, deben ser de la misma marca. En ese sentido la entidad requiere que tanto los computadores de escritorio y equipos portátiles sean de la misma casa fabricante. Los componentes internos que conforman la CPU deberán ser respaldados por la casa fabricante de los equipos de cómputo.

Cuando los equipos de cómputo e impresoras adquiridas sean de marca de fabricación extranjera, se deberá garantizar que el respaldo de repuestos y suministros en Colombia. Mínimo para cinco (5) años (Anexar documento).

Mantenimiento: Los usuarios no están autorizados para instalar o desinstalar dispositivos, o hacer mantenimiento a los equipos sin previa autorización de la Dirección de Sistemas de Información.

El Servidor Público que requiera soporte técnico debe dar aviso a la Dirección de Sistemas de Información para que allí el encargado envíe el personal especializado a diagnosticar el equipo; en caso que se presente un daño mayor el funcionario debe enviar el equipo con formato de requerimiento autorizado para que ingrese a mantenimiento correctivo.

Responsabilidad de la tenencia: El recurso tecnológico asignado será de uso exclusivo para labores propias de la Entidad y será responsabilidad del usuario que los retire de las instalaciones sin la respectiva autorización del jefe inmediato y registro de la novedad en la minuta de vigilancia.

Los Servidores Públicos a quienes se les asignen equipos de cómputo portátiles deberán adoptar las medidas de seguridad necesarias que garanticen la seguridad física del recurso tecnológico y salvaguardar la información.

Los servidores públicos deben dar aviso de inmediato al Almacén, de la pérdida o hurto del recurso tecnológico a su cargo, para que se surta el procedimiento establecido.

Los servidores públicos deben comunicar de manera inmediata a la Dirección de Sistemas de Información cuando detecte posibles riesgos por factores tales como humedad, inundaciones, choques eléctricos, robo, calentamientos etc.

Los Usuarios no deben consumir alimentos en áreas cercanas al recurso tecnológico.

La Dirección de Sistemas de Información será la responsable de Administrar las hojas de vida del recurso tecnológico, en la cual se registre todos los componentes con sus seriales, el software instalado con su número de licencia respectiva y además el registro de todos los mantenimientos realizados, tanto preventivos como correctivos.

Legalidad del Software: Todo software instalado en equipos de la Entidad, será autorizado o instalado por la Dirección de Sistemas de Información, la cual tiene autonomía para desinstalar o borrar software no autorizado, en desarrollo de actividades de control de uso de software legal.

Los Servidores públicos no deben instalar en los equipos de cómputo de propiedad de la Alcaldía, Software no autorizado por la Dirección de Sistemas de Información.

El servidor Público asumirá la responsabilidad por el software instalado en el computador que le sea asignado o que esté utilizando. Toda aplicación que esté instalada debe estar debidamente licenciada.

La Dirección de Sistemas de Información será la responsable del control e inventario de las licencias de software y del manejo de los medios de instalación.

Sistemas Operativos:

Aunque el sistema Operativo instalado en cada equipo esté configurado para realizar las actualizaciones automáticas, los usuarios de los equipos de cómputo serán los responsables de mantener actualizado el sistema operativo de su equipo, teniendo la precaución de no descargar las actualizaciones de sitios no seguros.

Los equipos servidores o los que hagan sus veces, deben contar con el software para realizar el chequeo de integridad del sistema operativo y del hardware. La periodicidad de su ejecución estará definida por la persona o la Dirección de Sistemas de Información designados para ello. Esto aplica para todos los equipos de cómputo (ej.: equipos de escritorio y portátiles)

Uso de servidores

Política: La Dirección de Sistemas de Información es la responsable de verificar la instalación y configuración de todo servidor que sea conectado a la red, y de implementar mecanismos de seguridad física y lógica.

Controles:

Ubicación de Servidores: Los servidores estarán ubicados en un área física que cumpla con las siguientes medidas de seguridad:

- El acceso debe ser restringido a personal autorizado
- La temperatura debe ser la adecuada para la cantidad de equipos
- Debe tener protección contra descargas eléctricas
- El mobiliario debe ser el adecuado
- Ubicación física en sitio libre de daño por humedad, goteras, inundaciones y demás efectos del clima.

Funcionalidad y mantenimiento de Servidores: Todo servidor que proporcione servicios a través de la red debe:

- Funcionar las 24 horas al día los 365 días del año
- Tener mantenimiento preventivo mínimo dos veces al año
- Hacerle revisión de su configuración anual
- Ser Monitoreado diariamente por la persona encargada por la Dirección de Sistemas de Información.

Control de accesos lógicos

Administración De Contraseñas Y Control De Acceso Lógico

Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas de información.

Política: Las tareas realizadas por los usuarios en cada uno de los sistemas de información de la Alcaldía de Madrid, serán controladas por medio de la creación de cuentas de usuario a los cuales se les controlarán los privilegios de acceso, modificación y eliminación, de conformidad con los roles y perfiles establecidos.

Controles:

Aprobaciones Requeridas para la Creación de Usuarios y Permisos: Para la creación, actualización o bloqueo de cuentas de usuario a los sistemas de información, las solicitudes para dichas actividades deben contener de forma clara y precisa la siguiente información

1. Nombre completo del funcionario
2. Correo electrónico Para notificación de Contraseñas.
3. Tipo de Permiso (Superadministrador, administrador, usuario según grado de privilegios.)
4. Tipo de vinculación: (Personal de Planta o Prestación de Servicios)
5. Si es personal de prestación de servicios, la fecha final del contrato
6. En caso de solicitar acceso a más de un aplicativo se debe especificar por cada uno de ellos los permisos a los que va a tener derecho
7. Los permisos deben ser solicitados por el director o secretario responsable de cada uno de los módulos.

Cambio Forzoso de Todas las Contraseñas del Administrador

Siempre que se detecte un ingreso no autorizado al sistema de información, los administradores del sistema deben cambiar inmediatamente cada una de sus contraseñas en el sistema.

Cambios de Contraseñas Periódicas para el Administrador

Todos los administradores deben cambiar periódicamente la contraseña en el sistema.

Control de Acceso al Sistema con Contraseña Individual para cada Usuario

Se precisa que el control de acceso al sistema, se debe realizar por medio de Usuario único, es decir que no se puede tener el acceso a la base de datos y otros recursos del sistema si no se encuentra privilegiado con uno.

La Dirección de Talento Humano reportará a la Dirección de Sistemas de Información el traslado o retiro de los servidores públicos, a fin de ejercer control sobre el estado de los usuarios.

La vigencia del usuario y contraseñas a personal de contrato estará sujeta a la fecha de finalización del contrato, siendo responsabilidad de los jefes inmediatos reportar a la Dirección de Sistemas de Información la novedad de retiro.

Longitud de la Contraseña de Usuario

Se debe tener en la longitud de las contraseñas un mínimo de ocho caracteres y una longitud máxima de cuatrocientos cincuenta y seis (456) caracteres, siendo esta una combinación de mayúsculas, minúsculas, números y un carácter especial.

Entrega de Contraseñas a Usuarios

Las contraseñas no se divulgan por medio de líneas telefónicas, se envían por correo electrónico, y el usuario debe cambiarla de manera inmediata al ingresar por primera vez al aplicativo.

Confidencialidad de las contraseñas

Se precisa que las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Hacerlo expone al usuario a responsabilizarse de acciones que otras personas hagan con su cuenta.

Los servidores públicos serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia la darán a conocer a otras personas, o harán uso de contraseñas ajenas, ni de la opción de autoguardado de contraseñas.

Cambio de contraseña cuando se sospecha que ha sido descubierta

Ante la posibilidad o sospecha de la perdida de confidencialidad de la contraseña, esta debe ser cambiada de manera inmediata y reportada el evento a la Dirección de Sistemas de Información.

Cambio de Contraseñas Periódicas para los usuarios en el Sistema

Se precisa que todos los usuarios cambien periódicamente la contraseña en el sistema y en el correo institucional mínimo una vez al año.

Restricción de horarios

Se implementará control de acceso a los aplicativos, en horarios autorizados por los líderes de los procesos propietarios de la información, de tal forma que, si se requiere el ingreso en horario adicional al señalado, debe mediar autorización escrita del director o Secretario de Despacho, indicando la hora de inicio, finalización y los días que debe estar autorizado.

Bloqueo por intentos

Los intentos fallidos de acceso al sistema de información antes del límite de tres intentos, despliegan un mensaje de advertencia indicando que el usuario no ha podido iniciar sesión debido a los datos de usuario o password son incorrectos. Cuando los intentos fallidos superan el máximo de tres, se desplegará un mensaje de bloqueo de usuario, lo que implica que debe comunicarse con el administrador del sistema para el desbloqueo respectivo.

Cerrar Sesión:

Todos los usuarios deben cerrar sesión cuando no van a hacer más uso del aplicativo, o cuando van a abandonar su estación de trabajo.

Administración de usuarios.

Los Administradores de los sistemas de información, deben revisar con una periodicidad mínima mensual, los derechos de acceso de los usuarios, con el fin de actualizar el estado de los mismos ocasionado por trasladados y retiros de la Entidad.

El uso de programas de acceso remoto será restringido y controlado por la Dirección de Sistemas de Información, y solo podrán autorizar su utilización los líderes dueños de los procesos mediante comunicación escrita, especificando el tiempo de utilización, las actuaciones a realizar y la justificación.

Para la instalación y uso de programas de acceso remoto, el usuario autorizado debe garantizar que el acceso remoto se realizará en un equipo seguro, libre de virus, programas maliciosos y espías.

Control de acceso físico

Política: El Ingreso al área de servidores y de procesamiento de información será restringido y controlado, y solo se autorizará con fines o propósitos esenciales por la Dirección de Sistemas de Información

Controles:

Toda actividad que se realice por terceros en las áreas de servidores y de procesamiento debe ser supervisada por el responsable de la Dependencia.

La Dirección de Sistemas de Información mantendrá un registro de todas las personas ajenas que ingrese a las áreas de servidores y de procesamiento de información, indicando, fecha, hora, nombre, actividad realizada, y nombre de quien autorizó.

Las Instalaciones de procesamiento de información administradas por la Alcaldía de Madrid se encontrarán separadas de las administradas por terceros.

Se debe impedir el ingreso a las áreas restringidas, de equipos de cómputo móvil, fotográfico, videos, dispositivos removibles o cualquier otro equipo que registre información, a menos que sea autorizado por el responsable de dicha área.

Seguridad física y del entorno

Política: Los equipos que hacen parte de la infraestructura tecnológica de la Alcaldía de Madrid, tales como servidores, estaciones de trabajo, centro de cableado, aires acondicionados, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

Controles:

Está prohibido fumar, beber o consumir alimentos en las áreas de servidores o cercanas a las estaciones de trabajo.

No está autorizado almacenar material peligroso, combustible e inflamable en sitios cercanos a las áreas de procesamiento o almacenamiento de información.

Disponibilidad del servicio

Política: La Entidad diseñará un plan de contingencia para garantizar la continuidad del servicio de los sistemas de información ante la DoS (Denegación de Servicios inesperados).

Controles

El plan de contingencia de los sistemas de información será diseñado y evaluado semestralmente por el Director de Sistemas de Información y los encargados de la seguridad de los sistemas de información.

La Entidad debe garantizar la disponibilidad de los recursos indicados en el plan de contingencia de los sistemas de información.

Registro y Auditoria

Política: Los sistemas de información que soporten los procesos críticos de la Alcaldía de Madrid, contarán con registros de auditoría de las actividades de usuario, de operación y administración del sistema.

Controles:

Los Log(Historial) de auditoría deben proporcionar información relevante para soportar procesos de auditoría y para contribuir al cumplimiento de las políticas de seguridad de la información.

Los líderes de los procesos propietarios de la información definirán los criterios a auditar de acuerdo con los requerimientos internos o externos o con los datos que considere sensibles a hechos fraudulentos.

El acceso a los logos de auditoría será restringido solo a los administradores del Sistema y a los propietarios de información o a quien estos autoricen por medios escritos.

Los administradores de los sistemas de información realizarán monitoreos trimestrales al log de auditoría, emitiendo un acta como evidencia de la actuación y reportando las presuntas irregularidades a los líderes de los procesos propietarios de la información.

ROLES Y RESPONSABILIDADES

Se deben formalizar cuáles son los roles y responsabilidades relacionados con seguridad de la información en la entidad (esto puede incluir diferentes áreas y funcionarios).
Comúnmente se definen responsabilidades a los siguientes roles o áreas:

- Alta Dirección
- Dirección de Sistemas de Información
- Control Interno
- Líderes de Proceso
- Responsable de Seguridad Digital
- Funcionarios

GESTIÓN DE LA POLÍTICA

Es importante indicar cómo será la gestión de la política a través de los siguientes puntos:

• Aprobación de la política.
• Difusión de la política.
• Revisión o Actualización de la política (Mínimo 1 vez cada 12 meses).
• Evaluación del cumplimiento de la política.

7. REGISTROS DE REFERENCIA

Las políticas de seguridad han sido formuladas teniendo como referencia la Norma NTC-ISO/IEC 27001, la Evaluación de Riesgos Administrativos y el modelo de seguridad de la información para la estrategia de Gobierno en Línea del Mintic.

Decreto 2573 de 2014: “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”

Ley 1273 de 2009: “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Ley 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.

Ley 1712 de 2014: “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

8. CUADRO DE REVISIÓN

Revision Número	DESCRIPCIÓN	FECHA	ELABORÓ		REVISÓ	
			CARGO	VoBo	CARGO	VoBo
01	Elaboración inicial del documento	13/09/2018	Yohana Marcela Garzón Castiblanco Profesional Universitario		Jorge Emilio Gaitán Berrios Secretario de Planeación Angélica Rojas Bermúdez Directora de Sistemas de Información.	