MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN

VERSIÓN 1.0

AYUNTAMIENTO MUNICIPAL EL CERCADO
CÓDIGO INSTITUCIONAL: 7025
RNC: 430004792

Índice

Introducción

El presente manual tiene como propósito establecer las políticas y procedimientos que regirán el uso de las Tecnologías de la Información y Comunicación (TIC), la gestión de la información, y el acceso a datos públicos en el Ayuntamiento Municipal de El Cercado. Este documento proporciona un marco normativo para garantizar que las operaciones del ayuntamiento se realicen de manera eficiente, transparente y segura, cumpliendo con las leyes dominicanas y las normativas sobre TIC. Además, establece las directrices para proteger la integridad de la información y mejorar la calidad de los servicios que se ofrecen a los ciudadanos.

El manual es aplicable a todo el personal del Ayuntamiento Municipal de El Cercado, independientemente de su nivel jerárquico o departamento. Las políticas y procedimientos aquí descritos cubren todos los aspectos relacionados con:

- El uso, administración y control de las TIC en el Ayuntamiento.
- La seguridad de la información y su confidencialidad.
- La disponibilidad de la información pública según la Ley 200-04 sobre Libre Acceso a la Información Pública.
- La digitalización y conservación de documentos.
- La planificación y ejecución de proyectos tecnológicos.

El alcance del manual incluye no solo a los empleados permanentes del ayuntamiento, sino también a los contratistas, proveedores y cualquier tercero que acceda a los sistemas de información del Ayuntamiento.

La implementación de las políticas y procedimientos descritos en este manual aportará los siguientes beneficios al Ayuntamiento Municipal de El Cercado:

1. **Mejora en la eficiencia administrativa**: A través de la correcta gestión de las TIC, se optimizarán los procesos internos, permitiendo una toma de decisiones más ágil y efectiva.
2. **Mayor transparencia**: La implementación de políticas claras sobre el acceso a la información pública aumentará la confianza de los ciudadanos en la gestión municipal.
3. **Seguridad de la información**: Las políticas sobre protección de datos garantizarán que la información sea manejada de manera segura, minimizando riesgos de acceso no autorizado o pérdida de datos.
4. **Cumplimiento normativo**: El manual asegura que el Ayuntamiento cumpla con las normativas nacionales, incluyendo la **NORTIC A1:2014**, la **Ley 200-04**, y otras legislaciones pertinentes, evitando sanciones legales.
5. **Mejora en la calidad de los servicios**: Al adoptar tecnologías de la información, el Ayuntamiento podrá ofrecer mejores servicios en línea, facilitando la interacción con los ciudadanos y la resolución de sus solicitudes de manera más rápida.

Misión

El Ayuntamiento Municipal de El Cercado tiene como misión promover el desarrollo integral de la comunidad, asegurando la transparencia, la eficiencia en la gestión de los recursos, y fomentando la participación ciudadana. Nos comprometemos a ofrecer servicios públicos de calidad a través de la utilización de tecnologías de la información y comunicación (TIC) y a garantizar el acceso equitativo a la información.

Visión

Ser un ayuntamiento líder en la República Dominicana en la implementación de TIC y en la prestación de servicios eficientes, transparentes y accesibles.

Aspiramos a transformar la administración pública local mediante el uso de plataformas tecnológicas que faciliten la interacción con los ciudadanos y mejoren la calidad de vida de nuestra comunidad.

Valores

- **Transparencia:** Garantizar la claridad en la gestión de los recursos públicos.
- **Responsabilidad:** Cumplir con el deber de proteger y gestionar los bienes y recursos de la comunidad.
- **Innovación:** Fomentar la modernización y uso de TIC en los procesos administrativos.
- **Accesibilidad:** Facilitar el acceso a los servicios y la información pública a todos los ciudadanos.
- **Participación ciudadana:** Involucrar a la comunidad en las decisiones y actividades del ayuntamiento.

Marco Legal

El funcionamiento del ***Ayuntamiento Municipal de El Cercado*** se encuentra regulado por una serie de leyes y normativas nacionales que aseguran la transparencia, eficiencia y seguridad en la gestión pública. A continuación, se detallan las principales leyes y decretos que deben ser observados en la implementación de las políticas y procedimientos establecidos en este manual.

Leyes y Normativas que Regulan el Funcionamiento del Ayuntamiento

1. **NORTIC A1:2014 – Norma General sobre el Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano**

Esta normativa establece las directrices para el uso adecuado de las TIC en las instituciones gubernamentales. Su propósito es garantizar la estandarización de

los procesos y plataformas tecnológicas, mejorando la gestión pública y asegurando la interoperabilidad entre los organismos del Estado. El ***Ayuntamiento Municipal de El Cercado*** debe cumplir con esta norma para garantizar la correcta implementación de las TIC, la seguridad de la información y la transparencia en la gestión.

2. Ley 200-04 sobre Libre Acceso a la Información Pública

Esta ley garantiza el derecho de los ciudadanos a acceder a la información pública gestionada por las instituciones del Estado. El Ayuntamiento Municipal de El Cercado tiene la obligación de proporcionar acceso a la información solicitada de manera transparente y oportuna. La Ley 200-04 establece que la información debe estar disponible para los ciudadanos sin restricciones, excepto en casos donde la confidencialidad esté protegida por otras normativas. El Ayuntamiento deberá implementar plataformas digitales, como portales web, para facilitar el acceso público a documentos e informes de gestión.

3. Ley 53-07 contra Crímenes y Delitos de Alta Tecnología

Esta ley regula la protección de los sistemas informáticos y tecnológicos utilizados en la administración pública. El ***Ayuntamiento Municipal de El Cercado*** debe implementar medidas de seguridad adecuadas para proteger la infraestructura tecnológica, los datos y la información de posibles ataques o accesos no autorizados. La ley sanciona delitos como el acceso ilegal a sistemas, la manipulación de datos, y otros crímenes tecnológicos que afecten la seguridad de la información pública.

4. Ley 107-13 sobre Derechos de las Personas en sus Relaciones con la Administración Pública

La Ley 107-13 regula los derechos de los ciudadanos en su interacción con las instituciones públicas. Esta ley garantiza que los ciudadanos puedan acceder a una buena administración, recibir un trato justo, y tener acceso a la información sobre los procedimientos administrativos que les afecten. El Ayuntamiento debe

asegurar que todos los ciudadanos puedan interactuar con la administración de manera clara, eficiente y accesible.

5. Decreto 694-09 – Sistema 311 de Denuncias, Quejas y Reclamaciones

El Decreto 694-09 establece el Sistema 311, que permite a los ciudadanos presentar denuncias, quejas y reclamaciones contra las instituciones públicas. El ***Ayuntamiento Municipal de El Cercado*** deberá tener un enlace directo al sistema 311 en su portal web para que los ciudadanos puedan reportar cualquier irregularidad en la gestión municipal. Además, se deberán establecer mecanismos para la atención rápida y efectiva de las reclamaciones recibidas.

6. Ley 126-02 sobre Comercio Electrónico, Documentos y Firma Digital

Esta ley regula el uso de las transacciones electrónicas y la validez legal de los documentos electrónicos y las firmas digitales en la República Dominicana. El ***Ayuntamiento Municipal de El Cercado*** deberá implementar procesos digitales que cumplan con esta normativa, garantizando que los documentos electrónicos emitidos tengan la misma validez que los documentos en formato físico, y que las firmas digitales sean seguras y verificables.

Otras normativas y decretos a considerar:

1. **Ley 340-06 sobre Compras y Contrataciones de Bienes, Servicios y Obras con Modificación de la Ley 449-06**

   Esta ley regula los procesos de compras y contrataciones en el sector público. El ***Ayuntamiento Municipal de El Cercado*** deberá cumplir con las disposiciones sobre contratación pública, asegurando transparencia y legalidad en la adquisición de bienes y servicios.

2. **Ley 42-2000 sobre Discapacidad en la República Dominicana**

Garantiza el acceso igualitario a servicios públicos para personas con discapacidades, incluyendo el acceso a información y la interacción con plataformas electrónicas del ayuntamiento.

Cumplimiento Normativo

El ***Ayuntamiento Municipal de El Cercado*** se compromete a cumplir con las leyes y normativas mencionadas en este manual, garantizando una gestión eficiente, transparente y en concordancia con el marco legal vigente en la República Dominicana. La falta de cumplimiento de estas normativas puede derivar en sanciones legales y en la pérdida de confianza pública.

Políticas Generales

Las políticas generales establecen las normas fundamentales que guían la gestión de las Tecnologías de la Información y Comunicación (TIC) en el ***Ayuntamiento Municipal de El Cercado***. Estas políticas están alineadas con la ***NORTIC A1:2014***, que establece directrices específicas para el uso de las TIC en la administración pública de la República Dominicana. La implementación de estas políticas asegura el uso eficiente y seguro de las TIC, mejorando la prestación de servicios y la transparencia en la gestión pública.

Normas Generales sobre el Uso e Implementación de las TIC (basado en NORTIC A1:2014)

1. Implementación de TIC en el Ayuntamiento

El ***Ayuntamiento Municipal de El Cercado*** deberá implementar las TIC de manera que optimicen los procesos internos, mejoren la interacción con los ciudadanos y garanticen la transparencia en la gestión pública. La infraestructura

tecnológica debe ser adecuada y suficiente para soportar las operaciones diarias del ayuntamiento, asegurando la continuidad de los servicios.

La implementación de las TIC debe:

- Ser accesible para todos los departamentos del ayuntamiento.
- Ser compatible con las plataformas y sistemas utilizados por otras instituciones del Estado.
- Asegurar la protección de la información y la confidencialidad de los datos.

2. Uso Responsable de las TIC

Todos los empleados del Ayuntamiento son responsables del uso adecuado de los recursos tecnológicos, incluyendo computadoras, software, sistemas de gestión, y acceso a redes. El uso de las TIC debe estar orientado a apoyar las funciones del ayuntamiento y ofrecer mejores servicios a los ciudadanos.

Se prohíbe el uso personal o no autorizado de los sistemas de TIC del Ayuntamiento, así como la instalación de software sin licencia o programas no aprobados por el Departamento de Tecnologías de la Información.

3. Seguridad de las TIC

El ***Ayuntamiento Municipal de El Cercado*** debe asegurar la protección de su infraestructura tecnológica y la información que maneja. Esto incluye:

- La implementación de controles de acceso para evitar el uso no autorizado de los sistemas.
- La realización de copias de seguridad periódicas de los datos para asegurar su disponibilidad en caso de fallos.
- La actualización continua de sistemas y software para prevenir vulnerabilidades de seguridad.

4. Formación Continua del Personal

Se establecerán programas de formación continua para el personal del ayuntamiento con el fin de mejorar sus habilidades en el uso de las TIC. Este entrenamiento deberá estar orientado a asegurar que los empleados puedan manejar correctamente los sistemas de gestión y las plataformas tecnológicas necesarias para realizar sus funciones.

5. Acceso a la Información Pública

De acuerdo con la ***Ley 200-04***, el Ayuntamiento se compromete a garantizar el acceso a la información pública. Para esto, se implementarán plataformas tecnológicas que permitan a los ciudadanos acceder a documentos, informes, y otra información de manera transparente y accesible.

El acceso a la información deberá ser gestionado de manera tal que se proteja la confidencialidad de los datos sensibles, asegurando el cumplimiento de las normativas vigentes en materia de privacidad y protección de datos.

Acceso a la Información Pública

El ***Ayuntamiento Municipal de El Cercado*** reconoce el derecho fundamental de los ciudadanos a acceder a la información pública, tal y como lo establece la ***Ley 200-04*** sobre Libre Acceso a la Información Pública. Este derecho es esencial para garantizar la transparencia en la gestión pública, promover la rendición de cuentas y fortalecer la confianza de los ciudadanos en las instituciones gubernamentales. A continuación, se detallan las normas y procedimientos relacionados con el acceso a la información pública en el ayuntamiento.

Normas sobre el Acceso a la Información Pública (Ley 200-04)

1. Derecho de Acceso

Según la ***Ley 200-04***, todo ciudadano tiene derecho a acceder a la información pública, entendida como cualquier información generada o recibida por el Ayuntamiento en el ejercicio de sus funciones. El acceso a esta información es gratuito y no requiere justificación por parte del solicitante.

2. Transparencia Activa

El Ayuntamiento está obligado a publicar proactivamente la información de carácter público en su portal de transparencia, incluyendo:

- Estructura organizacional y funciones del ayuntamiento.
- Informes financieros y presupuestarios.
- Proyectos, programas y actividades del ayuntamiento.
- Contrataciones y adquisiciones públicas.
- Resultados de auditorías y evaluaciones de desempeño.
- Otras informaciones de relevancia para la ciudadanía.

Esta información debe actualizarse periódicamente para garantizar que los datos sean actuales y accesibles.

3. Excepciones al Acceso

La Ley establece ciertas limitaciones al derecho de acceso, como:

- Información clasificada como confidencial por razones de seguridad o privacidad.
- Información que ponga en riesgo la seguridad nacional o pública.
- Datos personales protegidos por la legislación vigente.

Estas excepciones están detalladas en el Artículo 17 de la ***Ley 200-04*** y deberán ser aplicadas de manera estricta y justificada por el Ayuntamiento.

4. Responsabilidad de las Autoridades

El Ayuntamiento debe designar una ***Oficina de Acceso a la Información Pública*** (OAI), la cual será responsable de procesar y responder a las solicitudes de acceso a la información. Esta oficina estará encargada de:

- Recibir y tramitar las solicitudes de acceso a la información.
- Asegurar la disponibilidad de la información publicada en el portal de transparencia.
- Orientar a los ciudadanos sobre el derecho de acceso a la información.

Procedimientos de Solicitudes de Acceso a la Información

1. Recepción de la Solicitud

Los ciudadanos pueden realizar solicitudes de acceso a la información a través de los siguientes canales:

- **Presencial:** En las oficinas del Ayuntamiento Municipal de El Cercado.
- **En línea:** A través del portal de transparencia del ayuntamiento o mediante correo electrónico habilitado para este fin.
- **Teléfono:** Usando los números de contacto oficiales para recibir solicitudes de información.

La solicitud debe contener:

- Nombre completo y datos de contacto del solicitante.
- Descripción clara y precisa de la información solicitada.
- Medio preferido para recibir la información (correo electrónico, físico, etc.).

2. Plazos de Respuesta

El Ayuntamiento tiene un plazo de ***15 días hábiles*** para responder a la solicitud de información. En casos excepcionales, este plazo podrá extenderse por ***10 días hábiles adicionales***, informando al solicitante de las razones para la demora.

3. Entrega de la Información

La información solicitada será entregada en el formato solicitado (digital o impreso) de manera gratuita, a menos que los costos de reproducción o envío físico de los documentos requieran un pago mínimo. En cualquier caso, el solicitante será notificado previamente sobre los posibles costos.

4. Negativa de Información

Si la solicitud de acceso a la información es rechazada, el solicitante recibirá una respuesta por escrito detallando las razones de la negativa, las cuales deben basarse en los criterios legales establecidos en la ***Ley 200-04***. El solicitante tendrá derecho a presentar un recurso de revisión ante el mismo Ayuntamiento o ante los tribunales, conforme a lo dispuesto en la ley.

5. Mecanismos de Revisión y Quejas

En caso de que el solicitante no esté conforme con la respuesta recibida, puede interponer un recurso de revisión ante el Ayuntamiento o elevar una queja formal ante el Tribunal Superior Administrativo. Asimismo, los ciudadanos pueden utilizar el ***Sistema 311*** para presentar quejas relacionadas con la falta de acceso a la información pública.

6. Divulgación Proactiva de la Información

Además de responder a solicitudes específicas, el Ayuntamiento está obligado a divulgar proactivamente información pública a través de:

- **Portales web:** Información actualizada sobre las actividades del Ayuntamiento, gestión presupuestaria, y contrataciones.
- **Publicaciones periódicas**: Boletines informativos o informes anuales de gestión disponibles en línea o en formato impreso.

Beneficios del Sistema de Acceso a la Información Pública

El sistema de acceso a la información pública implementado por el ***Ayuntamiento Municipal de El Cercado*** tiene múltiples beneficios para los ciudadanos y la gestión municipal:

- **Mayor Transparencia**: Facilita que los ciudadanos conozcan en detalle cómo se gestionan los recursos públicos y se desarrollan los proyectos municipales.
- **Fomento de la Participación Ciudadana:** Al tener acceso a la información, los ciudadanos están mejor informados y pueden participar activamente en la vida pública y en las decisiones municipales.
- **Mejora de la Confianza Pública:** La transparencia en la gestión fortalece la confianza de la comunidad en las autoridades municipales y su capacidad de gestionar los recursos de manera adecuada.

Seguridad de la Información

La ***seguridad de la información*** es una prioridad para el ***Ayuntamiento Municipal de El Cercado***, dado que la protección de los datos y la información es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información que se maneja. Las directrices establecidas en esta sección se basan en la ***NORTIC A1:2014***, específicamente en su Sección 6.01, que establece las normativas para la seguridad de las TIC en el sector gubernamental.

Directrices para Garantizar la Seguridad de los Datos y la Información

1. Confidencialidad

El Ayuntamiento se compromete a proteger toda información confidencial bajo su control. Solo el personal autorizado tendrá acceso a los datos sensibles. Esto incluye información personal de los ciudadanos, documentos financieros, datos internos del ayuntamiento y cualquier otra información clasificada como confidencial.

2. Integridad de la Información

Se adoptarán medidas para garantizar que la información no sea alterada de forma no autorizada. Todo cambio en los sistemas de información del Ayuntamiento deberá ser registrado, y solo el personal debidamente autorizado podrá hacer modificaciones en los datos.

3. Disponibilidad de la Información

Se implementarán mecanismos que aseguren que la información esté disponible cuando se necesite, especialmente para las funciones críticas del Ayuntamiento. Esto incluye la implementación de planes de respaldo y recuperación de datos para asegurar que la información pueda ser recuperada en caso de incidentes o fallos técnicos.

4. Cumplimiento de Normas y Políticas

El Ayuntamiento adoptará las normas establecidas en la **NORTIC A1:2014**, así como otras normativas nacionales e internacionales sobre la seguridad de la información. Se evaluará periódicamente el cumplimiento de estas normas y se ajustarán las políticas internas de seguridad para mantenerse alineadas con las mejores prácticas.

Políticas de Manejo de la Información y Control de Acceso

1. Control de Acceso a los Sistemas de Información

El acceso a los sistemas de información del Ayuntamiento estará restringido a personal autorizado. Cada empleado recibirá un ***nombre de usuario*** y ***contraseña*** únicos para acceder a los sistemas, y los niveles de acceso serán otorgados de acuerdo con las responsabilidades y funciones de cada empleado.

- Los controles de acceso incluirán:
- Autenticación mediante credenciales seguras.
- Registros de acceso para monitorear quién accede a los sistemas y qué actividades realiza.
- Políticas de uso de contraseñas, que incluyen requisitos mínimos de longitud, complejidad y caducidad regular.

2. Gestión de la Información Sensible

Toda la información clasificada como sensible o confidencial será almacenada en sistemas seguros y protegidos mediante ***cifrado*** cuando sea necesario. La información sensible incluye:

- Datos personales de los ciudadanos.
- Información financiera del Ayuntamiento.
- Documentos internos relacionados con la gestión administrativa.

El uso de esta información estará limitado a las personas que tengan un motivo justificado para acceder a ella. Además, se deberá garantizar que no se comparta ni divulgue dicha información sin la autorización correspondiente.

3. Política de Uso del Correo Electrónico y Redes

El correo electrónico institucional y las redes internas del Ayuntamiento deben ser utilizadas únicamente para actividades relacionadas con las funciones

del Ayuntamiento. Está prohibido el uso de estos sistemas para fines personales o no autorizados. Los correos electrónicos enviados a través del sistema del Ayuntamiento que contengan información sensible deberán ser cifrados o protegidos mediante mecanismos de seguridad adecuados.

4. Política de Respaldo de Información

El Ayuntamiento implementará un ***sistema de respaldo periódico*** de toda la información crítica. Estos respaldos deberán realizarse de manera automática, y las copias de seguridad deberán almacenarse en ubicaciones seguras, fuera del lugar donde se originan los datos, para prevenir la pérdida en caso de desastres o incidentes mayores.

Las políticas de respaldo deberán cubrir:

- **Frecuencia de respaldo:** Diaria, semanal o según lo requerido por la naturaleza de los datos.
- Almacenamiento seguro de los respaldos.
- Procedimientos de restauración de la información en caso de pérdida de datos.

Responsabilidad de los Empleados Públicos en la Protección de la Información (NORTIC A1: Sección 6.01)

1. Responsabilidad Individual

Cada empleado es responsable de garantizar la seguridad de la información bajo su control. Esto incluye el manejo adecuado de contraseñas, la protección de los dispositivos electrónicos que contengan información del Ayuntamiento, y la notificación inmediata de cualquier incidente o sospecha de acceso no autorizado.

2. Cumplimiento de las Políticas de Seguridad

Todos los empleados deben seguir estrictamente las políticas de seguridad establecidas en este manual y en la **NORTIC A1:2014**. Cualquier incumplimiento de estas políticas será considerado una falta grave y podrá resultar en sanciones disciplinarias, que podrían incluir la terminación del empleo.

3. Capacitación en Seguridad de la Información

El Ayuntamiento proporcionará formación periódica a todos los empleados sobre las mejores prácticas de seguridad de la información, incluyendo:

- Cómo proteger las contraseñas y credenciales de acceso.
- Cómo identificar y evitar ataques informáticos, como phishing o malware.
- Buenas prácticas para el manejo de información confidencial.

4. Reporte de Incidentes de Seguridad

Los empleados están obligados a reportar inmediatamente cualquier incidente de seguridad que ponga en riesgo la información del Ayuntamiento. Esto incluye accesos no autorizados, pérdida de dispositivos, intentos de phishing, o cualquier actividad sospechosa relacionada con la seguridad de los sistemas.

Todos los incidentes deberán ser reportados al **Departamento de Tecnologías de la Información**, que será responsable de tomar las medidas correctivas necesarias y reportar el incidente a las autoridades competentes cuando sea necesario.

Plan de Acción en Caso de Violación de la Seguridad de la Información

En caso de que se detecte una violación de la seguridad de la información, se implementarán los siguientes pasos:

- **Contención inmediata del incidente:** El sistema afectado será aislado para evitar la propagación de la amenaza.
- **Investigación del incidente:** El equipo de TIC investigará la causa y el alcance del incidente para tomar medidas correctivas.
- **Restauración de los sistemas:** Se utilizarán las copias de seguridad para restaurar los datos y volver a la operación normal.
- **Informe del incidente:** Se elaborará un informe detallado sobre el incidente, incluyendo las lecciones aprendidas y las acciones tomadas para prevenir futuros incidentes.

Política de Uso de Tecnologías

El ***Ayuntamiento Municipal de El Cercado*** establece esta política de uso de tecnologías con el fin de regular el uso adecuado de las Tecnologías de la Información y la Comunicación (TIC) en sus operaciones. Estas políticas están basadas en las directrices de la ***NORTIC A1:2014***, específicamente en la Sección 2.03, que establece las normativas para la implementación, administración y uso de las TIC en el sector gubernamental.

Políticas para el Uso de TIC

1. Uso Responsable de las TIC

Las TIC del Ayuntamiento (computadoras, sistemas de gestión, redes, correos electrónicos, etc.) deben ser utilizadas exclusivamente para actividades relacionadas con las funciones del Ayuntamiento.

Los empleados están prohibidos de utilizar los recursos tecnológicos del Ayuntamiento para actividades personales o cualquier otro propósito no autorizado.

Queda prohibida la instalación de software no autorizado o sin licencia en los equipos del Ayuntamiento.

2. Prohibición del Uso Inadecuado de las TIC

El uso de las TIC para la divulgación de información no autorizada o confidencial está estrictamente prohibido. Todo el personal debe garantizar que la información sensible esté protegida.

El acceso a sitios web no relacionados con el trabajo, como aquellos que promuevan actividades ilegales, contenido inapropiado o que consuman ancho de banda de forma excesiva, está prohibido.

Cualquier actividad que comprometa la seguridad de la información o exponga al Ayuntamiento a riesgos cibernéticos será sancionada.

3. Control y Monitoreo de las TIC

El ***Departamento de Tecnologías de la Información*** tendrá la autoridad para monitorear el uso de los sistemas tecnológicos del Ayuntamiento con el fin de asegurar el cumplimiento de esta política.

Se registrarán y auditarán las actividades realizadas en los sistemas tecnológicos para detectar usos indebidos o no autorizados.

4. Mantenimiento y Actualización de los Sistemas

Los sistemas tecnológicos del Ayuntamiento deberán ser actualizados y mantenidos periódicamente por el ***Departamento de Tecnologías de la Información***. Esto incluye la actualización de software, sistemas operativos y medidas de seguridad para prevenir fallos o vulnerabilidades.

Los usuarios no deberán manipular ni modificar las configuraciones de los equipos o software sin la autorización previa del Departamento de TIC.

5. Responsabilidad de los Usuarios

Cada empleado es responsable del uso adecuado de las TIC a su disposición. El personal deberá proteger sus contraseñas, credenciales y

dispositivos tecnológicos, asegurando que no sean accesibles a personas no autorizadas.

El personal deberá reportar inmediatamente cualquier anomalía, incidente de seguridad o mal funcionamiento de los sistemas al Departamento de TIC.

Implementación de Software y Licencias (NORTIC A1: Sección 2.03)

1. Uso de Software Licenciado

El ***Ayuntamiento Municipal de El Cercado*** solo utilizará ***software con licencias válidas y legítimas***, de acuerdo con las normativas establecidas por la ***NORTIC A1:2014***. Está prohibido el uso de software pirata, sin licencia o software libre que no cumpla con los requisitos de seguridad y normativas legales.

El ***Departamento de Tecnologías de la Información*** será responsable de la adquisición, instalación y gestión de todo el software utilizado en el Ayuntamiento. Cualquier necesidad de software por parte de los empleados deberá ser solicitada a este departamento para su evaluación y aprobación.

2. Selección de Software

La selección del software utilizado por el Ayuntamiento deberá basarse en criterios como:

- Cumplimiento con las normativas vigentes (NORTIC, Leyes de Propiedad Intelectual, Ley 126-02 sobre Comercio Electrónico).
- Compatibilidad con los sistemas y plataformas tecnológicas del Ayuntamiento.
- Seguridad y protección de los datos.
- Costos de adquisición y mantenimiento.

- Se promoverá el uso de ***software libre*** cuando sea adecuado para las funciones administrativas y cumpla con los requisitos de seguridad y funcionalidad.

3. Actualización y Mantenimiento de Software

El ***Departamento de TIC*** será responsable de realizar las actualizaciones necesarias de los programas utilizados, asegurando que el software esté protegido contra vulnerabilidades de seguridad y funcionando con el mejor rendimiento.

Todo software deberá ser actualizado a su última versión cuando esté disponible, y se realizarán copias de seguridad antes de proceder a la actualización, para asegurar la integridad de los datos.

4. Desinstalación de Software No Autorizado

Cualquier software que se encuentre instalado en los equipos del Ayuntamiento sin la autorización o licencia correspondiente será desinstalado inmediatamente por el ***Departamento de TIC***. El uso de software no autorizado o ilegal está prohibido y puede ser sancionado de acuerdo con las políticas del Ayuntamiento y la ley.

5. Auditoría de Licencias

El Departamento de TIC realizará auditorías periódicas para asegurar que todo el software utilizado esté debidamente licenciado y cumpla con las normativas legales.

En caso de detectar incumplimientos en el uso de licencias, se tomarán medidas correctivas y se reportará a las autoridades competentes si fuera necesario.

6. Capacitación en el Uso de Software

El ***Ayuntamiento Municipal de El Cercado*** proporcionará capacitación continua a los empleados sobre el uso adecuado del software instalado en los

sistemas del ayuntamiento. Esta capacitación incluirá la correcta utilización de las herramientas tecnológicas y la conciencia sobre la seguridad y los riesgos informáticos asociados al mal uso de software no autorizado.

Cumplimiento de las Políticas

El incumplimiento de estas políticas de uso de tecnologías puede resultar en sanciones disciplinarias, que varían desde advertencias hasta la terminación del empleo, dependiendo de la gravedad del caso. Además, se podrán aplicar sanciones legales en casos de uso indebido de software sin licencia, de acuerdo con las normativas de la ***Ley 53-07*** contra Crímenes y Delitos de Alta Tecnología y la ***Ley 126-02*** sobre Comercio Electrónico y Firma Digital.

Infraestructura Tecnológica

La infraestructura tecnológica del ***Ayuntamiento Municipal de El Cercado*** es clave para asegurar la continuidad operativa, la seguridad de la información y la eficiencia en la prestación de servicios. Esta sección resume las directrices esenciales para la gestión y mantenimiento de la infraestructura tecnológica, basadas en el ***Capítulo 4 de la NORTIC A1:2014***.

Directrices sobre la Infraestructura Tecnológica y su Mantenimiento (NORTIC A1: Capítulo 4)

1. Evaluación y Planificación de la Infraestructura

El Ayuntamiento debe realizar evaluaciones periódicas de su infraestructura tecnológica para asegurarse de que los sistemas sean adecuados y puedan soportar las operaciones y demandas actuales y futuras.

Toda adquisición de nuevos equipos tecnológicos o la actualización de infraestructura deberán estar alineada con los planes estratégicos de TIC y ser evaluada por el ***Departamento de Tecnologías de la Información***.

2. Mantenimiento Preventivo

Se implementarán ***planes de mantenimiento preventivo*** para todos los equipos tecnológicos (servidores, computadoras, sistemas de red) con el fin de evitar fallos inesperados. Esto incluye la revisión periódica de hardware, la limpieza física de los equipos y la actualización de los sistemas operativos y software.

3. Gestión de Inventarios de TIC

Se deberá llevar un control detallado de todos los activos tecnológicos, como servidores, computadoras y dispositivos de red. Estos inventarios ayudarán a asegurar que todo el equipo esté correctamente mantenido y actualizado, y a planificar futuras adquisiciones.

Administración de la Red de Área Local (LAN), Conectividad y Servidores

1. Red de Área Local (LAN)

La **red LAN** del Ayuntamiento debe garantizar una conectividad segura y estable entre todos los dispositivos de la organización. La red debe ser gestionada por el ***Departamento de TIC***, quien será responsable de:

- Configurar el acceso y las credenciales para los usuarios.
- Monitorear el tráfico de red para evitar congestión o accesos no autorizados.
- Implementar cortafuegos y sistemas de detección de intrusiones para garantizar la seguridad.

2. Conectividad a Internet

El Ayuntamiento debe garantizar una conexión a internet de alta calidad y seguridad, con ancho de banda suficiente para soportar las actividades diarias y la interacción con plataformas externas, como los portales de transparencia y servicios a los ciudadanos.

El acceso a internet debe ser monitoreado y controlado para evitar el uso indebido y garantizar que los recursos de conectividad se usen de manera eficiente.

3. Servidores

Los ***servidores*** del Ayuntamiento alojan datos sensibles y sistemas críticos. Se deben implementar las siguientes medidas para garantizar su funcionamiento:

- **Respaldo regular:** Todos los servidores deben tener copias de seguridad regulares, preferiblemente en ubicaciones externas, para garantizar la disponibilidad de los datos en caso de fallos o desastres.
- **Actualización de sistemas:** Los servidores deben actualizarse regularmente para corregir vulnerabilidades de seguridad y mejorar el rendimiento.
- **Monitoreo constante:** Se implementarán herramientas de monitoreo para detectar fallos en los servidores y tomar medidas correctivas de manera inmediata.

Gestión de Proyectos de TIC

La ***gestión de proyectos de Tecnologías de la Información y Comunicación (TIC)*** en el ***Ayuntamiento Municipal de El Cercado*** sigue principios claros para asegurar que todos los proyectos tecnológicos sean eficaces, cumplan con los plazos, y optimicen los recursos. Basado en las directrices de la ***NORTIC A1:2014***, estos son los puntos clave:

1. Planificación del Proyecto

Cada proyecto de TIC debe tener un plan detallado, que incluya los objetivos, el alcance, el presupuesto, los recursos requeridos y un cronograma.

El ***Departamento de TIC*** es responsable de supervisar la planificación y asegurarse de que el proyecto esté alineado con los objetivos estratégicos del Ayuntamiento.

2. Selección de Proveedores

Los proyectos que requieren la adquisición de software o servicios externos deben seguir los procedimientos de ***licitación pública*** y cumplir con las normativas de compras públicas (Ley 340-06).

Se evaluarán criterios como la calidad, costo y compatibilidad con la infraestructura tecnológica existente.

3. Supervisión y Control

Durante la ejecución del proyecto, se debe llevar a cabo un ***monitoreo continuo*** para garantizar que el proyecto avance según lo planificado. Esto incluye:

- Revisión de hitos importantes.
- Control del presupuesto y los recursos.
- Gestión de riesgos.

4. Entrega y Evaluación

Una vez completado, se evaluará el proyecto para garantizar que cumpla con los requisitos especificados. Esto incluye pruebas del sistema, validación de resultados y la capacitación del personal que usará la nueva tecnología.

Se documentará todo el proceso, y se implementará un plan de ***soporte y mantenimiento*** para garantizar la sostenibilidad del proyecto a largo plazo.

Digitalización de Documentos

La ***digitalización de documentos*** es un proceso esencial para mejorar la eficiencia administrativa y garantizar la conservación a largo plazo de la información. El

Ayuntamiento Municipal de El Cercado sigue las directrices establecidas en el ***Capítulo 7.01 de la NORTIC A1:2014***, que regula la digitalización de documentos oficiales y su adecuado almacenamiento.

Procedimientos para la Digitalización y Conservación de Documentos Oficiales

1. Selección de Documentos para Digitalización

Se priorizarán para digitalización los documentos que sean críticos para las operaciones del Ayuntamiento, incluyendo:

- Actas oficiales.
- Documentos financieros.
- Registros de gestión pública y administrativa.
- Documentos históricos de relevancia.

2. Proceso de Digitalización

La digitalización debe realizarse utilizando ***equipos de escaneo de alta calidad*** para asegurar que los documentos sean legibles y precisos. Los documentos digitalizados deberán cumplir con los formatos estandarizados, preferiblemente en ***PDF/A***, que es apto para la conservación a largo plazo.

Se deberá garantizar que los documentos digitalizados sean fieles a sus originales y que no sufran modificaciones durante el proceso.

3. Almacenamiento y Organización

Los documentos digitalizados serán almacenados en sistemas de gestión documental seguros que permitan el fácil acceso y recuperación de la información cuando sea necesario.

Se implementarán ***índices*** y ***etiquetas*** adecuadas para la organización y clasificación de los documentos, facilitando la búsqueda eficiente.

4. Respaldo de Documentos Digitalizados

Todos los documentos digitalizados deberán tener ***copias de respaldo*** almacenadas en ubicaciones diferentes para prevenir la pérdida de información en caso de fallos o desastres.

Se implementarán sistemas automáticos de ***respaldo diario*** para garantizar que la información esté protegida.

5. Acceso y Seguridad

El acceso a los documentos digitalizados estará limitado a personal autorizado. Se implementarán ***medidas de control de acceso***, como contraseñas y registros de auditoría, para garantizar la seguridad de la información digitalizada.

Los documentos sensibles deberán ser encriptados antes de su almacenamiento.

6. Conservación a Largo Plazo

Los documentos digitalizados que sean parte del archivo histórico del Ayuntamiento o que tengan valor legal deben ser conservados indefinidamente.

Se realizarán ***auditorías periódicas*** para asegurar que los documentos digitalizados siguen siendo accesibles y que los medios de almacenamiento continúan siendo adecuados.

Control de Inventarios de TIC

El ***Control de Inventarios de Tecnologías de la Información y Comunicación (TIC)*** es crucial para garantizar una administración eficiente de los recursos tecnológicos del ***Ayuntamiento Municipal de El Cercado***. Este control asegura que todos los activos tecnológicos sean gestionados de manera efectiva, manteniendo un registro claro de su ubicación, estado y uso.

Procedimientos para el Control de Inventarios de TIC

1. Registro Detallado de Activos

Se debe llevar un ***registro detallado*** de todos los equipos y dispositivos tecnológicos, incluyendo computadoras, servidores, impresoras, escáneres, dispositivos de red, y software.

El registro deberá contener información clave como:

- Descripción del equipo.
- Número de serie.
- Fecha de adquisición.
- Ubicación.
- Usuario responsable.
- Estado actual (operativo, en mantenimiento, etc.).

2. Mantenimiento del Inventario

El inventario deberá ser actualizado de forma periódica para reflejar cualquier cambio en el estado de los activos, como nuevas adquisiciones, bajas, o equipos en reparación.

Las ***auditorías de inventario*** deberán realizarse al menos una vez al año para verificar la existencia y estado de todos los equipos.

3. Clasificación de Equipos por Prioridad

Los equipos serán clasificados según su ***importancia operativa***, lo que permitirá una mejor planificación de su mantenimiento y actualización. Los equipos críticos (servidores, equipos de red, etc.) recibirán mayor atención en cuanto a su mantenimiento y respaldo.

4. Etiquetado y Control Físico

Todos los activos tecnológicos deberán estar etiquetados con un ***código de identificación único***, que permita su fácil rastreo y gestión. Las etiquetas deberán estar vinculadas al sistema de inventario digital para facilitar la búsqueda de información.

5. Responsabilidad de los Usuarios

Cada usuario será responsable de los equipos que se le asignen. En caso de que el equipo sufra daños, pérdida o cualquier alteración, el usuario deberá notificar al ***Departamento de TIC*** para tomar las medidas adecuadas.

6. Gestión de Software

Además del inventario físico, se llevará un control del ***software instalado*** en cada equipo, asegurando que todas las licencias sean legales y vigentes.

El Departamento de TIC será responsable de gestionar las licencias de software y de garantizar que no se utilicen programas sin licencia.

7. Baja y Eliminación de Activos

Los equipos que hayan llegado al final de su vida útil serán retirados del inventario mediante un proceso de baja formal, que incluirá la eliminación segura de cualquier información contenida en el dispositivo antes de su disposición.

Los equipos dados de baja serán gestionados conforme a las políticas de ***desecho electrónico seguro***.

Gestión de Incidentes

La ***Gestión de Incidentes*** en el ***Ayuntamiento Municipal de El Cercado*** se enfoca en la identificación, análisis y resolución rápida de cualquier incidente relacionado con las Tecnologías de la Información y Comunicación (TIC). Esto

asegura la continuidad operativa y minimiza el impacto de fallos o ataques en los sistemas tecnológicos.

Procedimientos para la Gestión de Incidentes

1. Identificación de Incidentes

Un incidente se define como cualquier evento inesperado que afecte la seguridad, disponibilidad o funcionalidad de los sistemas TIC del Ayuntamiento. Esto puede incluir:

- Ataques cibernéticos (phishing, malware, etc.).
- Fallos en hardware o software.
- Interrupciones en el servicio de red o internet.
- Pérdida o robo de dispositivos.

Todos los empleados tienen la responsabilidad de ***reportar inmediatamente*** cualquier incidente al ***Departamento de Tecnologías de la Información (TIC)***.

2. Registro y Clasificación

Los incidentes serán ***registrados*** en un sistema centralizado que documente la naturaleza del incidente, el tiempo de ocurrencia, el personal afectado y el impacto.

Se clasificarán según su ***nivel de gravedad*** (bajo, medio, alto) para priorizar su resolución. Los incidentes críticos, como los que afecten la seguridad de los datos o interrumpan operaciones clave, recibirán la máxima prioridad.

3. Análisis y Diagnóstico

El Departamento de TIC será responsable de realizar un ***análisis detallado*** del incidente para identificar la causa raíz y el alcance del problema.

El diagnóstico incluirá:

- Identificación de los sistemas o datos afectados.
- Evaluación de posibles riesgos o daños.
- Recomendación de medidas correctivas.

4. Respuesta y Resolución

Una vez identificado el incidente, se tomarán medidas correctivas para restaurar el sistema o la información afectada. Estas acciones pueden incluir:

- Restauración desde copias de seguridad.
- Implementación de parches o actualizaciones de software.
- Bloqueo de accesos no autorizados o eliminación de malware.

Los incidentes críticos deben resolverse en el menor tiempo posible para minimizar el impacto en las operaciones.

5. Comunicación y Notificación

Durante el proceso de gestión de incidentes, se mantendrá una ***comunicación clara y oportuna*** con los empleados afectados y las autoridades del Ayuntamiento.

Los incidentes de alto nivel que puedan comprometer la seguridad pública o la privacidad de los ciudadanos serán notificados a las autoridades competentes.

6. Registro de Soluciones

Una vez resuelto el incidente, se registrarán las acciones tomadas y los resultados obtenidos. Esto es crucial para documentar las lecciones aprendidas y prevenir incidentes similares en el futuro.

7. Evaluación y Mejora Continua

Se realizará una evaluación posterior al incidente para analizar la respuesta y detectar áreas de mejora. Este análisis ayudará a actualizar los protocolos de seguridad y fortalecer los sistemas.

Se implementarán medidas preventivas para reducir la probabilidad de que el mismo tipo de incidente ocurra nuevamente.

Plan de Continuidad y Disponibilidad

El ***Plan de Continuidad y Disponibilidad*** del ***Ayuntamiento Municipal de El Cercado*** tiene como objetivo garantizar que los servicios y sistemas tecnológicos esenciales puedan seguir funcionando o ser restaurados rápidamente ante cualquier interrupción, ya sea causada por desastres naturales, fallos técnicos o incidentes de seguridad. Este plan sigue las mejores prácticas recomendadas en la ***NORTIC A1:2014***.

Directrices del Plan de Continuidad y Disponibilidad

1. Identificación de Servicios Críticos

El primer paso es identificar los sistemas, servicios y datos que son esenciales para el funcionamiento del Ayuntamiento, tales como:

- Sistemas de gestión administrativa y financiera.
- Portales de transparencia y servicios al ciudadano.
- Servidores de correo electrónico y comunicaciones.

Estos sistemas serán priorizados en caso de cualquier interrupción para asegurar su restauración rápida.

2. Estrategia de Respaldo

El respaldo regular de datos es fundamental para garantizar que la información crítica pueda ser recuperada en caso de pérdida. Los respaldos se realizarán diariamente y se almacenarán tanto en ubicaciones locales como externas (fuera del sitio) para mayor seguridad.

Los respaldos deben incluir:

- Datos operativos (documentos, bases de datos).
- Configuraciones de sistemas y redes.
- Software y aplicaciones claves.

3. Planes de Recuperación ante Desastres

Se implementará un ***Plan de Recuperación ante Desastres (DRP)*** que cubra todos los escenarios posibles, como fallos de hardware, ataques cibernéticos, incendios o inundaciones. Este plan debe incluir:

- Procedimientos claros para restaurar los sistemas desde copias de seguridad.
- Equipos de emergencia y centros de datos alternativos que puedan ser activados en caso de desastres mayores.

El ***Departamento de TIC*** será responsable de liderar la recuperación de los sistemas siguiendo este plan.

4. Acceso Remoto y Alternativas Operativas

Se establecerán mecanismos que permitan a los empleados acceder de manera **remota y segura** a los sistemas críticos del Ayuntamiento en caso de que las instalaciones principales no sean operativas.

El Ayuntamiento contará con un ***sitio alternativo*** donde se puedan realizar operaciones esenciales mientras se restauran los sistemas principales.

5. Pruebas y Simulaciones

Se realizarán simulacros regulares para poner a prueba el Plan de Continuidad y evaluar la capacidad de respuesta ante interrupciones. Estos simulacros identificarán posibles fallos en el plan y permitirán realizar mejoras.

Los resultados de las pruebas serán documentados, y se actualizarán las estrategias y procedimientos según sea necesario.

6. Comunicación en Situaciones de Emergencia

Se establecerán protocolos de comunicación interna y externa para informar rápidamente a los empleados y ciudadanos sobre cualquier interrupción y las medidas que se están tomando para restaurar los servicios.

La comunicación será clara, proporcionando plazos estimados de restauración y acciones a seguir.

7. Revisión y Actualización

El Plan de Continuidad y Disponibilidad deberá ser revisado y actualizado anualmente, o después de cualquier incidente mayor, para asegurarse de que sigue siendo eficaz y alineado con las necesidades del Ayuntamiento.

Las revisiones incluirán la actualización de los sistemas críticos, los procedimientos de respaldo, y los contactos de emergencia.

Recomendaciones sobre Seguridad TIC

Las siguientes recomendaciones sobre ***Seguridad de las Tecnologías de la Información y Comunicación (TIC)*** están diseñadas para garantizar la protección de los sistemas y datos del ***Ayuntamiento Municipal de El Cercado.*** Estas medidas, basadas en las mejores prácticas y alineadas con la ***NORTIC A1:2014***, son fundamentales para prevenir riesgos y mejorar la capacidad de respuesta ante posibles amenazas.

Recomendaciones Clave sobre Seguridad TIC

1. Autenticación y Control de Accesos

Implementar un sistema de autenticación multifactor para todos los usuarios que acceden a sistemas críticos. Esto agrega una capa adicional de seguridad al exigir algo más que una contraseña (por ejemplo, un código temporal o una identificación biométrica).

Establecer ***niveles de acceso*** basados en los roles y responsabilidades de cada empleado. Solo los usuarios autorizados deben tener acceso a datos sensibles o sistemas clave.

2. Cifrado de Datos Sensibles

Todos los datos sensibles (como información personal, financiera o confidencial) deben estar ***cifrados*** tanto en tránsito como en reposo. Esto asegura que, en caso de una violación de seguridad, los datos sean ininteligibles para terceros no autorizados.

Utilizar ***protocolos de encriptación robustos***, como AES (Advanced Encryption Standard) para el cifrado de datos.

3. Actualización de Sistemas y Software

Garantizar que todos los sistemas, software y dispositivos utilizados por el Ayuntamiento estén ***actualizados*** con los últimos parches de seguridad. Las vulnerabilidades conocidas son uno de los principales puntos de entrada para ataques cibernéticos.

Implementar políticas que obliguen a realizar ***actualizaciones automáticas*** en cuanto estén disponibles.

4. Protección contra Malware y Amenazas Cibernéticas

Instalar y mantener ***software antivirus*** y ***antimalware*** en todos los dispositivos del Ayuntamiento. Este software deberá ser actualizado regularmente para defenderse contra las nuevas amenazas.

Implementar cortafuegos (firewalls) y sistemas de detección de intrusos que monitoreen el tráfico de red y alerten sobre comportamientos sospechosos.

5. Capacitación en Seguridad para el Personal

Realizar ***capacitaciones periódicas*** para todos los empleados sobre las mejores prácticas de seguridad cibernética. Esto incluye:

Identificación de correos electrónicos fraudulentos o ataques de phishing.

- Buenas prácticas de creación y gestión de contraseñas.
- Responsabilidad en el manejo de información sensible.

Los empleados deben saber cómo reaccionar ante un posible incidente de seguridad.

6. Política de Contraseñas

Implementar una política que exija el uso de ***contraseñas complejas*** (mínimo de caracteres, inclusión de mayúsculas, minúsculas, números y caracteres especiales).

Forzar el cambio regular de contraseñas (cada 60 o 90 días) y prohibir el uso de contraseñas repetidas.

Fomentar el uso de ***gestores de contraseñas*** para evitar que los empleados utilicen contraseñas débiles o las compartan de manera insegura.

7. Respaldo y Recuperación de Datos

Asegurar que se realicen ***copias de seguridad automática y regular*** de todos los sistemas críticos y datos importantes. Estas copias de seguridad deben estar protegidas y almacenadas en ubicaciones externas para su recuperación en caso de desastres.

Establecer un ***plan de recuperación*** que permita restaurar rápidamente los datos y sistemas en caso de incidentes graves.

8. Auditorías de Seguridad

Realizar ***auditorías periódicas de seguridad*** para identificar vulnerabilidades y verificar el cumplimiento de las políticas de seguridad del Ayuntamiento.

Las auditorías deben incluir pruebas de penetración para evaluar la resistencia de los sistemas ante ataques externos.

9. Política de Uso de Dispositivos Personales

Establecer una política clara sobre el uso de dispositivos personales (teléfonos móviles, laptops, etc.) en el trabajo, especialmente cuando se accede a sistemas o datos del Ayuntamiento.

Los dispositivos personales que se utilicen para acceder a los sistemas del Ayuntamiento deberán cumplir con las políticas de seguridad, incluidas las medidas de cifrado y antivirus.

10. Monitoreo Continuo de la Red

Implementar un sistema de ***monitoreo continuo*** que permita detectar y responder a actividades sospechosas en la red del Ayuntamiento en tiempo real.

Cualquier comportamiento anómalo, como intentos de acceso no autorizados o picos inusuales de tráfico, debe ser investigado inmediatamente.

Capacitación y Concientización

El ***Ayuntamiento Municipal de El Cercado*** reconoce la importancia de la ***capacitación y concientización*** en el uso adecuado y seguro de las Tecnologías de la Información y Comunicación (TIC). La formación continua de los empleados es fundamental para garantizar el uso eficiente de los recursos tecnológicos y la protección de la información.

Políticas de Capacitación y Concientización

1. Capacitación Inicial

Todo empleado nuevo del Ayuntamiento recibirá una ***capacitación inicial*** obligatoria sobre el uso de las TIC, que incluirá:

- Uso de los sistemas y plataformas tecnológicas internas.
- Normativas de seguridad y protección de datos.
- Procedimientos operativos para el manejo de documentos digitales y físicos.

La capacitación será coordinada por el ***Departamento de Tecnologías de la Información (TIC)*** y deberá completarse dentro del primer mes de empleo.

2. Capacitación Continua

Se realizarán sesiones de capacitación periódicas (al menos una vez al año) para actualizar a los empleados sobre nuevas herramientas tecnológicas, cambios en los sistemas, o actualizaciones de seguridad.

La capacitación incluirá temas como:

- Buenas prácticas de seguridad informática (gestión de contraseñas, protección contra phishing, etc.).
- Uso adecuado de los sistemas de gestión documental y herramientas digitales.

- Procedimientos de respuesta ante incidentes de seguridad.

3. Concientización sobre Seguridad Informática

Se implementarán ***campañas de concientización*** periódicas para recordar a los empleados la importancia de seguir las políticas de seguridad. Estas campañas incluirán:

- Envío de boletines informativos.
- Carteles y recordatorios en las áreas de trabajo sobre buenas prácticas de seguridad.
- Simulaciones de ataques cibernéticos (como pruebas de phishing) para evaluar la respuesta de los empleados y reforzar el aprendizaje.

4. Formación Específica por Departamento

Cada departamento recibirá capacitaciones específicas en función de las herramientas y sistemas que utilizan. Por ejemplo:

- El personal de finanzas recibirá formación adicional en la gestión de sistemas financieros y la seguridad de los datos financieros.
- Los encargados de la atención al público se capacitarán en el uso de sistemas para la gestión de solicitudes ciudadanas y el acceso a la información pública.

5. Capacitación en la Gestión de Incidentes

Todos los empleados recibirán formación sobre los procedimientos de respuesta a incidentes de seguridad. Esto incluirá:

- Cómo identificar un incidente de seguridad (accesos no autorizados, pérdidas de información, ataques de malware).
- A quién reportar el incidente y cómo proceder para minimizar el impacto.
- Procedimientos para recuperar la información en caso de pérdidas o ataques.

6. Monitoreo del Desempeño

El desempeño de los empleados en el uso de TIC y el cumplimiento de las políticas de seguridad será monitoreado continuamente. En casos donde se identifiquen deficiencias, se ofrecerá formación complementaria para mejorar el nivel de competencia tecnológica de los empleados.

7. Evaluación de la Capacitación

Después de cada sesión de capacitación, los empleados deberán completar una evaluación para garantizar que han comprendido los conceptos clave. Esta retroalimentación ayudará al Departamento de TIC a ajustar los programas de formación según sea necesario.

Se realizarán encuestas periódicas para identificar áreas donde los empleados sientan que necesitan más formación.

Revisión y Actualización del Manual

La ***Revisión y Actualización del Manual de Políticas y Procedimientos*** es un proceso fundamental para asegurar que el documento refleje siempre las mejores prácticas, esté alineado con los cambios tecnológicos, y cumpla con las normativas legales vigentes. La gestión continua del manual garantiza su relevancia y efectividad en la operación del ***Ayuntamiento Municipal de El Cercado.***

Periodicidad de la Revisión

El manual será revisado anualmente para asegurar que las políticas y procedimientos continúen siendo pertinentes y eficaces. Esta revisión incluirá la evaluación de nuevas tecnologías, actualizaciones legales y cambios en las operaciones internas del Ayuntamiento.

En caso de cambios significativos en las normativas TIC (como actualizaciones a la ***NORTIC*** u otras leyes aplicables), o la introducción de nuevos

sistemas tecnológicos, se realizará una revisión extraordinaria para reflejar estos cambios.

Proceso para Actualizar las Políticas y Procedimientos del Manual

Iniciación de la Revisión: El ***Departamento de Tecnologías de la Información (TIC)***, en conjunto con la administración del Ayuntamiento, será responsable de iniciar el proceso de revisión anual. Durante este proceso, se consultarán las áreas clave que utilizan o gestionan las TIC para identificar posibles mejoras o cambios necesarios.

Evaluación de Cambios y Recomendaciones: Cualquier empleado o departamento podrá sugerir cambios o actualizaciones al manual basados en su experiencia operativa o en el descubrimiento de áreas que requieran ajustes. Las sugerencias serán evaluadas por el Departamento de TIC y el equipo directivo del Ayuntamiento.

Análisis de Cumplimiento Normativo: Se revisarán las normativas y leyes vigentes, como la ***NORTIC A1:2014***, la ***Ley 200-04*** sobre el acceso a la información pública, y otras leyes relacionadas con la gestión de TIC y la protección de datos. El manual será ajustado para asegurar el cumplimiento con todas las regulaciones aplicables.

Revisión Técnica: Se analizarán los cambios tecnológicos implementados en el Ayuntamiento, asegurando que el manual refleje las últimas actualizaciones en infraestructura tecnológica, software, seguridad de la información y gestión de incidentes.

Aprobación de Cambios: Cualquier modificación propuesta será revisada por el ***equipo directivo*** del Ayuntamiento. Una vez aprobadas las actualizaciones, se procederá a la implementación de los cambios en el manual.

Difusión de las Actualizaciones: Las actualizaciones al manual serán comunicadas a todos los empleados mediante ***correos electrónicos***, ***reuniones informativas*** y la actualización de las versiones electrónicas del manual disponibles en los sistemas internos del Ayuntamiento. Se garantizará que todos los empleados estén al tanto de los nuevos procedimientos o políticas implementadas.

Capacitación sobre Nuevas Políticas: Cuando se introduzcan cambios significativos en las políticas o procedimientos, se proporcionará ***capacitación*** a los empleados para asegurar que comprendan y puedan cumplir con los nuevos lineamientos.

Documentación de los Cambios

Todos los cambios realizados al manual serán documentados y archivados. Cada nueva versión del manual deberá incluir un historial de revisiones que detalle las modificaciones realizadas, la fecha de implementación

Se mantendrán copias de las versiones anteriores del manual para referencia histórica y cumplimiento normativo.

Mecanismos de Retroalimentación

Se establecerán canales de retroalimentación para que los empleados puedan sugerir mejoras continuas a las políticas y procedimientos del manual. Estos canales incluyen encuestas, reuniones periódicas con los departamentos y buzones de sugerencias electrónicas.

Apéndices

Glosario de Términos

1. TIC (Tecnologías de la Información y Comunicación): Conjunto de herramientas y recursos tecnológicos que permiten la gestión,

almacenamiento, procesamiento y transmisión de información, esenciales para la operación del Ayuntamiento.

2. NORTIC A1:2014: Norma dominicana que regula el uso de TIC en las instituciones públicas para garantizar estandarización, seguridad y eficiencia en la administración de la información.

3. Ley 200-04: Ley de Libre Acceso a la Información Pública que otorga a los ciudadanos el derecho a acceder a información pública manejada por instituciones del Estado.

4. Ley 53-07: Ley contra Crímenes y Delitos de Alta Tecnología, que protege los sistemas informáticos del Estado contra ciberataques y delitos tecnológicos.

5.Seguridad de la Información: Prácticas y tecnologías utilizadas para proteger los datos contra accesos no autorizados, pérdida o alteración.

6. Cifrado: Proceso de codificación de la información para que solo usuarios autorizados puedan acceder a ella.

7. Respaldo: Copia de seguridad de los datos para restaurarlos en caso de pérdida o daño.

8. Autenticación Multifactor: Sistema de seguridad que requiere más de una forma de verificación para acceder a sistemas o datos.

9. Phishing: Tipo de ataque cibernético en el que los atacantes intentan obtener información confidencial (como contraseñas) mediante correos electrónicos o sitios web fraudulentos.

10. Sistema de Gestión Documental: Herramienta utilizada para almacenar, organizar y gestionar documentos digitales, asegurando su acceso y conservación.

Referencias Legales

Este manual se fundamenta en las siguientes leyes, decretos y normativas, las cuales regulan el uso de Tecnologías de la Información y Comunicación (TIC) y la gestión pública en la República Dominicana:

1. **NORTIC A1:2014**: Norma General sobre el Uso e Implementación de las TIC en el Estado Dominicano.

2. **Ley 200-04:** Ley de Libre Acceso a la Información Pública.

3. **Ley 53-07:** Ley sobre Crímenes y Delitos de Alta Tecnología.

4. **Ley 107-13:** Ley sobre los Derechos de las Personas en sus Relaciones con la Administración Pública.

5. **Ley 126-02:** Ley sobre Comercio Electrónico, Documentos y Firma Digital.

6. **Decreto 694-09:** Sistema 311 de Denuncias, Quejas y Reclamaciones.

7. **Ley 340-06:** Ley sobre Compras y Contrataciones de Bienes, Servicios y Obras.

8. **Ley 42-2000:** Ley sobre Discapacidad en la República Dominicana.