Córdoba, 12 JUL 2024

VISTO: *Las competencias funcionales dispuestas mediante Ordenanza N° 13.440.*

Y CONSIDERANDO:

QUE, *conforme lo establecido en el artículo 15 de la mencionada Ordenanza N° 13.440, es competencia de esta Secretaría de Ciudad Inteligente y Transformación Digital determinar las normas y estándares de aplicación obligatoria para todas las Secretarías y Organismos dependientes de la Municipalidad de la ciudad de Córdoba, referidos a sistemas de información, hardware, sistemas operativos, aplicaciones estándar y/o a medida, así como en la intervención, evaluación y asesoramiento general en la adquisición de recursos de hardware y software específicos para la red municipal.*

QUE, *asimismo, en consonancia con lo mencionado ut supra, y a efectos de evitar la diversidad en la adquisición de bienes y servicios y propender a una gestión unificada, mediante Decreto N° 54 de fecha 16 de enero de 2024, se determinaron los supuestos en los cuales corresponde la intervención previa de esta Secretaría.*

QUE, *en consecuencia, a lo expresado precedentemente y con el objetivo de definir pautas y mejores prácticas para el desarrollo, implementación y administración de los recursos, surge oportuno en esta instancia aprobar los estándares de Base de Datos, Desarrollo de Aplicaciones y Telecomunicaciones, así como las Políticas Generales de Infraestructura Tecnológica y de Seguridad.*

Por ello, la normativa citada y en uso de sus atribuciones;

EL SECRETARIO DE CIUDAD INTELIGENTE Y

TRANSFORMACIÓN DIGITAL

RESUELVE

Artículo 1º: APRUÉBANSE *a partir de la fecha de la presente Resolución, los "Estándares y Políticas Tecnológicas para la Transformación Digital", los que, como Anexo I compuesto de ochenta (80) fojas útiles, forma parte integrante de la presente Resolución, a los fines de su implementación en el ámbito de la Administración Pública Provincial.*

Artículo 2º: PROTOCOLÍCESE, *comuníquese, publíquese y archívese.*

021

12 JUL 2024

IGNACIO RAFAEL GEI
SECRETARIO DE CIUDAD INTELIGENTE
Y TRANSFORMACIÓN DIGITAL
MUNICIPALIDAD DE CÓRDOBA

Secretaría de
Ciudad Inteligente y
Transformación Digital

Municipalidad
de Córdoba

ANEXO I

021

Secretaría de
Ciudad Inteligente y
Transformación Digital

Municipalidad
de Córdoba

Estándar de Base de Datos

MUNICIPALIDAD DE CÓRDOBA

SECRETARÍA DE CIUDAD INTELIGENTE Y TRANSFORMACIÓN DIGITAL

SUBSECRETARÍA DE INFRAESTRUCTURA TECNOLÓGICA Y CONECTIVIDAD

021

Título	ESTÁNDAR DE BASE DE DATOS				
Resumen	Este documento describe estándar de base de datos de la Municipalidad de Córdoba.				
Tipo	Estándar	**Versión**	1.0	**Código**	EST-001

Nivel de circulación:	Público.
Clasificación	No Confidencial. Propiedad de la Municipalidad de Córdoba.

Ciclo de Aprobación			
	Nombre	**Posición/Cargo**	**Fecha**
Revisado	Alejandro Gomez	Jefatura de Infraestructura	01/07/2024
Revisado	Facundo N. Oliva Cúneo	Director de Ciberseguridad	01/07/2024
Aprobado	Gustavo Saravia	Subsecretario de Infraestructura Tecnológica y Conectividad	16/07/2024

Registro de cambios			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	10/06/2024	Valentina Parejo (Dir. de Interoperabilidad), Gonzalo Carena (Dir. Gral. de Gestión de Datos)	Creación del documento.

021

Contenido

021

1. Introducción

El presente documento establece un estándar técnico para el diseño e implementación de base de datos en el ámbito de la Municipalidad de Córdoba.

Un estándar (como lo define la ISO) "son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito". Ayudan a aclarar, guiar y controlar los procesos y actividades de TIC, y a crear un lenguaje común con el que los distintos actores (autoridades, personal técnico y usuarios internos, proveedores y ciudadanos en general) puede comunicarse claramente acerca de los necesidades, problemas y servicios relacionados o soportados por tecnologías informáticas y de comunicaciones (TIC's).

IMPORTANTE: Si en algún proyecto en particular se requiriera algún acuerdo diferente para alguno de los puntos detallados en este documento, o se requiriera un punto faltante en este documento, se debe contar con la aprobación de la Secretaría de Ciudad Inteligente y Transformación Digital para llevar adelante dicho o dichos puntos en el proyecto.

2. Objetivo

Este estándar tiene como objetivo definir pautas y mejores prácticas para desarrollar, implementar y administrar base de datos de manera efectiva, segura y escalable.

El propósito de este documento es servir como un compendio práctico y autorizado de estándares propuestos dentro del ámbito de la Municipalidad de Córdoba.

3. Alcance

Los estándares de Tecnología de Información y Comunicaciones se aplican a todas las dependencias y organismos auxiliares del Gobierno de la Municipalidad de Córdoba.

Este estándar se aplica a toda base de datos que se implemente en el ámbito de la Municipalidad de Córdoba.

4. Normativa de referencia

- Carta Orgánica Municipal de la Ciudad de Córdoba.
- Ordenanza N° 13440 del Consejo Deliberante de la Ciudad d Córdoba.
- Decreto N° 054-24 del Intendente de la Ciudad de Córdoba.

5. Autoridad

Los estándares de Tecnología de Información y Comunicaciones se publica bajo la

autoridad de la Secretaría de Ciudad Inteligente y Transformación Digital del Gobierno de la Municipalidad de Córdoba. Dicha Secretaría fija las directrices y normatividad en materia de TIC, guiando el enfoque de aplicación e implementación en todo el gobierno.

6. Generalidades

El control y responsabilidad de la información de la aplicación, debe estar a cargo de un organismo perteneciente al Gobierno de la Municipalidad de Córdoba. Toda persona que utiliza o tienen acceso a información del Gobierno de la Municipalidad de Córdoba, y a otros activos asociados, debe resguardar el grado de confidencialidad e integridad de la misma, y no afectar su disponibilidad, manteniendo en todo momento protegida la información y otros activos asociados.

Se deben considerar en el diseño, desarrollo e implementación, los aspectos referentes a la seguridad informática, los que se establecerán en cada caso y en forma conjunta con el área correspondiente Secretaría de Ciudad Inteligente y Transformación Digital.

7. Requerimientos de Base de Datos

Los puntos marcados con asterisco (*) deberán documentarse y entregarse a la Subsecretaría de Infraestructura Tecnológica y Conectividad para su aprobación

7.1 Motores de base de datos permitidos

- PostgreSQL: Versiones 14, 15, 16 (o superior).

Estos motores de bases de datos deben ser implementados sobre servicios: Relational Database Service (RDS) de la nube de Amazon Web Services (AWS) en la cuenta administrada por la Municipalidad de Córdoba.

Como alternativa, y solo en modalidad "on premise" en la Municipalidad de Córdoba:

- SQL Server: Versiones 2016, 2017, 2019, 2022 (o superior).

Al crear bases de datos se deberá especificar codificación UTF-8mb4 o en su defecto UTF-8.

7.2 Conexiones *

Las conexiones a la base de datos deben abrirse solo cuando sea necesario y cerrarse inmediatamente después de su uso. No se deben mantener conexiones abiertas de forma innecesaria, ya que esto puede afectar el rendimiento y la escalabilidad de la base de datos.

Se deben utilizar herramientas y técnicas adecuadas para gestionar las conexiones a la base de datos, así como también se debe monitorear el uso de las conexiones para identificar y resolver posibles cuellos de botella.

021

7.3 Diagrama de Entidad Relación *

Herramientas online: DBdiagrams.io, DrawSQL.app, sqlDBM.com, DBdesigner.net.

Aplicaciones: SQL Developer Data Modeler, Erwin versión 7.1.

7.4 Dimensionamiento de Recursos *

Se debe presentar estimaciones de:

- Cantidad de usuarios que utilizaran la aplicación.
- Cantidad de sesiones concurrentes.
- Espacio físico que ocuparan los datos:
    - Estimación del tamaño inicial de la base de datos en gigabytes (GB).
    - Estimación de la tasa de crecimiento mensual de la base de datos en porcentaje (%).
    - Volumen de datos futuro: Estimación del tamaño de la base de datos en un período futuro determinado (por ejemplo, 1 año, 2 años).

7.5 Entrega y Optimización de Consultas Principales

En algunos casos se puede requerir la entrega de las consultas principales ejecutadas en la aplicación o vistas del sistema para su análisis detallado y la correspondiente optimización (tuning).

7.6 Usuario / Usuario Referente *

Entrega de un listado de usuarios de la aplicación, identificados por DNI, CUIL y nombre completo. Se debe designar a uno de ellos como referente de la aplicación, quien actuará como el responsable de atender consultas relacionadas con la base de datos

7.7 Sobre la construcción de aplicaciones

Los esquemas que pidan ser creados deben dar soporte a aplicaciones WEB. No se permiten aplicaciones de escritorio.

7.8 Acceso a datos

Encapsular la capa de datos dentro de una capa de acceso a datos (DAO) que ofrezca una interfaz claramente definida para la capa de negocios. Esta capa de DAO puede emplear procedimientos almacenados, consultas SQL dinámicas u otros métodos apropiados para acceder a los datos. La interacción entre la capa de negocios y la capa de DAO debe realizarse exclusivamente a través de esta interfaz, evitando así la dependencia directa de

los procedimientos almacenados

8. Estandarización de las estructuras de datos

Para todo desarrollo de aplicaciones se deberán tener en cuenta los siguientes requisitos de estandarización para las Estructuras de Datos a fines de:

- Garantizar la aplicación de un nivel mínimo de calidad en los sistemas de información.
- Proporcionar un enfoque consistente y un lenguaje común en entornos con múltiples equipos de desarrollo.
- Conseguir que los componentes de los sistemas de información sean fáciles de entender y mantener.
- Facilitar el proceso de introducción al nuevo personal de desarrollo.

8.1 Responsabilidades

Todos los miembros de los equipos de desarrollo deben:

- **Seguir y aplicar los estándares:** Se espera que todos los miembros del equipo comprendan y apliquen consistentemente los estándares de desarrollo establecidos.
- **Interpretar correctamente los estándares:** Es importante que cada miembro del equipo tenga la capacidad de interpretar correctamente los estándares y aplicarlos de manera adecuada en su trabajo diario.
- **Mantener actualizados los conocimientos sobre los estándares:** Se recomienda que los miembros del equipo se mantengan actualizados sobre cualquier cambio o revisión de los estándares de desarrollo.
- **Documentar las desviaciones de los estándares:** En caso de que una situación particular requiera una desviación de un estándar, se debe documentar claramente la justificación, el impacto potencial y la alternativa elegida.
- **Proponer mejoras a los estándares:** Se alienta a los miembros del equipo a identificar oportunidades para mejorar los estándares existentes y proponer cambios formalmente a través de los canales establecidos.

8.2 Nivel de redundancia

No se permitirá redundancia en la especificación del contenido de las tablas que conforman la estructura de la base de datos. Cada dato debe almacenarse en un solo lugar y no debe duplicarse en diferentes tablas. Esta norma tiene como objetivo principal mejorar la

021

integridad de los datos y reducir la complejidad de las consultas.

En caso de que sea necesario mejorar el rendimiento de la aplicación, se podrán utilizar estrategias de tipificación de datos, como la creación de índices o la normalización de las tablas. Sin embargo, la tipificación solo se debe utilizar como último recurso y siempre se debe considerar cuidadosamente su impacto en la complejidad del modelo de datos y el mantenimiento del mismo. Se recomienda limitar la tipificación a un máximo de cinco atributos por tabla.

8.3 Niveles alcanzados en normalización de las estructuras

Se requerirá, al menos, hasta la implementación de la Tercera Forma Normal en la construcción de las estructuras.

9. Nomenclatura de elementos de BD

9.1 Tablas

9.1.1 Diccionario De Datos Para Definición De Las Tablas

Cada tabla debe tener su comentario para especificar el objetivo de la misma.

9.1.2 Denominación

T (mayúscula) seguida de un _ (guión bajo): T_NOMBRE, en plural, que represente el contenido de la tabla. Ejemplo: T_FACTURAS

Si se trata de más de una palabra para representar el contenido separar a las mismas con _ (guiones bajos) y la segunda palabra debe ir en singular. Ejemplo: T_TIPOS_FACTURA

9.1.3 Características

- No tener tablas sin definición de clave primaria (primary key).
- Evitar tener tablas innecesarias en el sistema. Un buen diseño es uno simple.
- Se deben utilizar claves primarias subrogadas (campo único numérico, de caracteres o alfanumérico) en combinación con una clave alterna (que podría ser compuesta) que represente la unicidad de los objetos en la tabla.
- Deben incluirse atributos en las tablas, con fines de auditoría y traza de transacciones realizadas en los registros.

9.1.4 Registros históricos

En el caso de necesitar registrar el borrado físico de los registros, se deberán crear

tablas Históricas. Estas deben ser nombradas con el mismo nombre de la tabla de donde provienen los registros borrados anteponiendo T_HIST_(Nombre tabla).

Las tablas históricas se actualizarán a través de triggers.

9.2 Triggers

Un trigger es una rutina almacenada especial (procedimiento o función) que se ejecuta automáticamente en respuesta a eventos específicos de la base de datos, como la inserción, actualización o eliminación de datos en una tabla.

Cada trigger está asociado a una tabla específica y a un evento específico. El evento define cuándo se dispara el trigger, y la tabla define el contexto en el que se ejecuta el trigger.

Se requieren triggers de Insert, Update y Delete, para actualizar información de auditoria.

9.2.1 Denominación

TG_(nombre_tabla)_ACCION

Donde acción es:

- INS si el evento es un Insert.
- UPD si el evento es un Update.
- DEL si el evento es un Delete.

9.3 Vistas

9.3.1 Denominación

VT seguida de un _ (guión bajo): VT_NOMBRE, Nombre representativo de la información que muestre la vista. Ejemplo: VT_FACTURAS

9.4 Check / Constraint

9.4.1 Denominación

- CK_(tabla)_campo
- Ejemplo: CK_FAC_TFAC (check de la tabla FACTURAS del campo ID_TIPO_FACTURA)

9.5 Secuencias

021

12 JUL 2024

Se establecerán secuencias para cualquier identificador (ID) en una tabla que requiera almacenar números enteros únicos generados automáticamente. Para secuencias que necesiten valores consecutivos, como los números de factura, se definirán secuencias controladas por la aplicación.

9.5.1 Denominación

- SEQ_(nombre_tabla)
- Ejemplo: SEQ_FACTURAS

9.6 Constraint

9.6.1 Denominación

Constraint Clave primaria: La clave primaria es un conjunto de campos que identifica de forma única un registro en una tabla.

- Primary Key: PK_FACTURAS (clave primaria de la tabla Facturas)

Constraint Clave foránea: Las claves foráneas se emplean para establecer relaciones entre tablas vinculadas. Una clave foránea establece una conexión entre una o varias columnas de una tabla y la clave primaria de la tabla referenciada.

- Foreing Key: FK_FAC_TFAC (clave foránea a la tabla Tipos Facturas)
- Unique Contraint: UK_FAC_SUC (clave única de la tabla Facturas por la columna Sucursal)

9.7 Atributos

9.7.1 Diccionario De Datos Para Definición De Los Atributos

Cada columna debe tener su comentario para indicar su significado.

9.7.2 Denominación

Los campos de una tabla representan los atributos de una entidad y describen sus propiedades. Es crucial que los nombres de estos campos sean simples, representativos e intuitivos, de modo que se comprenda fácilmente su significado.

Es recomendable evitar abreviaciones en la medida de lo posible; en caso de ser necesarias, es importante documentarlas adecuadamente para garantizar su comprensión.

El nombre del campo clave de una tabla debe ser el nombre de la tabla, en singular seguido del sufijo ID_.

- ID_(identificador)

- Ejemplo: ID_ARTICULO

Para identificar el contenido del dato, se sugiere utilizar "N" seguida de un guion bajo (_) para separar el identificador:

- N_ (nombre/descripción) - Nombre, en singular, que represente el contenido del dato
- Ejemplo: N_ARTICULO

Si se trata de más de una palabra para representar el contenido separar las mismas con _ (guiones bajos): Ejemplo: ID_TIPO_ARTICULO

Los campos que representen la misma entidad del mundo real deben tener el mismo nombre en todas las tablas del esquema.

No se recomienda agregar sistemáticamente el nombre de la tabla o una abreviación como prefijo a todos los campos de una tabla. Esto puede introducir redundancia y complejidad innecesaria al sistema

9.8 Formatos

9.8.1 Formatos de Fecha

El formato debe ser dd/mm/yyyy. Para fechas completas dd/mm/yyyy hh24:mi:ss.

9.8.2 Idioma

Se requiere que todo texto (comentarios del programador en código fuente, descripciones de columnas de una tabla, nombres de columnas, etc) esté escrito exclusivamente en español y se desaconseja el uso del inglés en cualquier forma.

9.8.3 Características en Tipo y Extensión de los Atributos

Los tipos de datos definidos por el usuario ofrecen un mecanismo para garantizar la coherencia de los tipos de datos en la base de datos. Para su uso adecuado:

- Se debe identificar el tipo de dato necesario según los valores específicos que va a contener, como por ejemplo: Number(), Varchar(), Date, entre otros.
- Es necesario determinar la extensión mínima requerida para cada tipo de dato, por ejemplo: Number(4), Varchar(20), etc.
- Todos los campos de tipo Varchar deben ser insertados sin espacios antes ni después.
- Todos los textos que se almacenen deberán utilizar codificación UTF-8mb4 (Unicode Transformation Format – 8 bit – Multi Byte 4) o en su defecto UTF-8.

9.9 Obligatoriedad

La obligatoriedad de los atributos se define de la siguiente manera:

- Los atributos obligatorios se especifican como "Not Null".
- Aquellos que pueden aceptar valores nulos se definen como "Null".

Es importante evitar tener un exceso de columnas que puedan ser nulas en una tabla, ya que esto puede indicar un esquema poco o nada normalizado. La falta de normalización puede ocasionar problemas de consistencia en los datos, ya que un mismo campo podría terminar almacenándose en varias tablas.

Sin embargo, es crucial encontrar un equilibrio entre la normalización y el rendimiento de la base de datos. Excesiva normalización puede resultar en una pérdida de rendimiento en ciertas operaciones. Por lo tanto, es necesario ajustar el nivel de normalización según los requisitos específicos de cada proyecto. Como regla general, la tercera forma normal suele ser un buen punto intermedio que equilibra la estructura de la base de datos y el rendimiento

9.10 Índices

Los índices son un recurso fundamental para mejorar la eficiencia en la localización y acceso de registros dentro de una tabla en una base de datos. Opcionalmente, pueden garantizar la unicidad de los valores del índice. Sin embargo, es importante tener en cuenta que mientras los índices benefician los tiempos de consulta de registros, también pueden ralentizar las operaciones de inserción y actualización en los campos indexados.

Es crucial considerar la conveniencia de crear índices en diversas situaciones:

- Sobre las columnas que conforman cada clave foránea de una tabla, con el fin de facilitar las operaciones de unión (joins). Esto permite optimizar las consultas que involucran múltiples tablas y mejorar el rendimiento general de la base de datos al reducir el tiempo necesario para unir conjuntos de datos.
- Sobre columnas utilizadas en consultas frecuentes o en cláusulas "WHERE" complejas en sentencias SQL. Al indexar estas columnas, se aceleran las búsquedas y se reduce el tiempo necesario para recuperar los registros que cumplen con los criterios de búsqueda. Esto es especialmente útil en casos donde las consultas son intensivas en términos de recursos y se ejecutan con frecuencia.
- En situaciones donde se requiera ordenar las filas de una tabla con regularidad. La creación de índices en las columnas utilizadas para ordenar los resultados de consultas puede mejorar significativamente el rendimiento de las operaciones de clasificación, ya que reduce el tiempo necesario para recuperar los datos en el orden deseado.

9.10.1 Denominación

- IDX_(tabla)_columna/s
- Ejemplo: IDX_FAC_TFAC (índice de la tabla T_FACTURAS por la columna ID_TIPO_FACTURA). Se determinan los 3 primero caracteres para el nombre de la tabla, obviando la letra T inicial, y de las columnas.

En el caso de la columna ID_TIPO_FACTURA se coloca solo la T de tipos y las 3 primeras letras de la siguiente palabra. Y en el caso ID_ESTADO_TRAMITE se coloca E de estados y las 3 primeras letras de la siguiente palabra. Para columnas con más de una palabra, colocar las 3 primeras letras de cada palabra.

9.11 Variables / Parámetros

9.11.1 Denominación

Cuando las variables o parámetros corresponden a columnas de una tabla, deben ser nombrados de la misma manera que la columna. Para los parámetros recibidos, se recomienda utilizar el prefijo "p_", mientras que, para los valores obtenidos de una consulta, se sugiere utilizar el prefijo "v_". Esto ayuda a clarificar la procedencia y el propósito de cada variable o parámetro en el código, facilitando la comprensión y el mantenimiento del mismo.

Ejemplo:

- p_nombre_columna: representa un parámetro recibido que corresponde a la columna "nombre_columna".
- v_valor_columna: representa un valor obtenido de una consulta que corresponde a la columna "valor_columna".

9.12 Procedimientos Almacenados

Los procedimientos almacenados son una herramienta poderosa para encapsular lógica de negocio y mejorar el rendimiento de las aplicaciones de bases de datos. Seguir buenas prácticas en su desarrollo puede ayudar a crear procedimientos eficientes, mantenibles y fáciles de leer.

Es fundamental seguir algunas prácticas recomendadas al trabajar con los procedimientos almacenados:

- **Declaración de procedimientos:** Es importante utilizar bloques BEGIN/END para encapsular el código de cada procedimiento. Esto mejora la claridad, la organización y la legibilidad del código.
- **Uso de mayúsculas y minúsculas:** Se recomienda utilizar mayúsculas para todas las palabras clave, identificadores y nombres de objetos, mientras que los textos

entrecomillados deben ir en minúsculas. Esta convención facilita la lectura y el mantenimiento del código.

- **Evitar utilizar SELECT *:** En lugar de usar **SELECT *** para recuperar todas las columnas de una tabla, se debe listar explícitamente las columnas necesarias. Esto ayuda a independizar la sentencia de cambios en la estructura de la tabla. Limitar el uso de la notación SELECT * a casos excepcionales, como en situaciones donde se utiliza la función COUNT o dentro de un cursor que recupere datos de una fila en una variable de registro (rowtype)

9.12.1Denominación

- PR_NOMBRE
- Ejemplo: PR_REGISTROS_VENTA

9.13 Funciones

Las funciones definidas por el usuario son un recurso que permite incorporar lógica dentro de la base de datos, utilizando un lenguaje de scripting que extiende el SQL estándar.

9.13.1Denominación

- FC_NOMBRE
- Ejemplo: FC_VERIFICA_PORCENTAJES.

9.14 Paquetes (en caso de aplicar)

Incluyen funciones y procedimientos, así como declaraciones de datos propios.

9.14.1Denominación

- PCK_NOMBRE
- Ejemplo: PCK_CONTABILIDAD

9.15 Tablas Auxiliares

Nombre descriptivo de la tabla, según estandarización mencionada anteriormente.

Para cada tabla auxiliar, se debe mantener un diccionario de datos que incluya:

- **Definición de campos:** Una breve descripción del contenido de cada campo, detallando su propósito y naturaleza.

- **Referencia a las tablas asociadas:** En caso de que exista una relación con otras tablas, se debe especificar la naturaleza de esta relación para facilitar la comprensión del esquema de la base de datos.
- **Detalle del contenido de cada tabla auxiliar:** Esto implica un análisis exhaustivo para ajustar los aspectos de normalización y garantizar la coherencia y eficiencia del diseño de la base de datos.

9.16 Excepciones y manejo de errores

El manejo de excepciones y errores en bloques de código SQL es fundamental para asegurar la integridad y fiabilidad de las aplicaciones en cualquier motor de base de datos. Se deben seguir las siguientes prácticas:

- **Previsión de errores:** Es crucial anticipar todos los posibles errores que pueda generar un bloque de código y reservar el uso de cláusulas genéricas para controlar errores inesperados.
- **Información detallada de errores:** Al manejar excepciones, se debe proporcionar al usuario final un mensaje claro y comprensible junto con cualquier código de error relevante, facilitando así la identificación y resolución del problema. Además, se puede incluir información adicional dirigida al desarrollador, como el código de error interno y enlaces con recursos de ayuda.
- **Excepciones definidas por el usuario:** Todas las excepciones definidas por el usuario deben ser manejadas adecuadamente en los procedimientos correspondientes, garantizando así un control efectivo de los errores personalizados.
- **Declaración explícita de excepciones:** Cada posible condición de error durante la ejecución normal del programa debe tener una excepción declarada explícitamente, permitiendo un manejo preciso de los flujos de ejecución y una respuesta adecuada ante cualquier situación inesperada.
- **Excepciones para errores funcionales o advertencias:** Es esencial definir excepciones específicas para manejar errores de tipo funcional o condiciones de advertencia, asegurando una respuesta coherente y apropiada en todas las situaciones.

021

ING. GUSTAVO E. SARAVIA
Subsecretario de Infraestructura
Tecnológica y Conectividad
Secretaría Ciudad Inteligente
y Transformación Digital

Secretaría de
Ciudad Inteligente y
Transformación Digital

Municipalidad
de Córdoba

Estándar de Desarrollo de Aplicaciones

MUNICIPALIDAD DE CÓRDOBA

SECRETARÍA DE CIUDAD INTELIGENTE Y TRANSFORMACIÓN DIGITAL

SUBSECRETARÍA DE INFRAESTRUCTURA TECNOLÓGICA Y CONECTIVIDAD

Título	ESTÁNDAR DE DESARROLLO DE APLICACIONES				
Resumen	Este documento describe estándar de desarrollo de aplicaciones de la Municipalidad de Córdoba.				
Tipo	Estándar	**Versión**	1.0	**Código**	EST-002

Nivel de circulación:	Público.
Clasificación	No Confidencial. Propiedad de la Municipalidad de Córdoba.

Ciclo de Aprobación			
	Nombre	**Posición/Cargo**	**Fecha**
Revisado	Facundo N. Oliva Cúneo	Director de Ciberseguridad	01/07/2024
Aprobado	Gustavo Saravia	Subsecretario de Infraestructura Tecnológica y Conectividad	16/07/2024

Registro de cambios			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	10/06/2024	Valentina Parejo (Dir. de Interoperabilidad), Gonzalo Carena (Dir. Gral. de Gestión de Datos)	Creación del documento.

Contenido

021

1. Introducción

El presente documento establece un estándar técnico para el diseño y desarrollo de aplicaciones en el ámbito de la Municipalidad de Córdoba.

Un estándar (como lo define la ISO) "son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito". Ayudan a aclarar, guiar y controlar los procesos y actividades de TIC, y a crear un lenguaje común con el que los distintos actores (autoridades, personal técnico y usuarios internos, proveedores y ciudadanos en general) puede comunicarse claramente acerca de los necesidades, problemas y servicios relacionados o soportados por tecnologías informáticas y de comunicaciones (TIC's).

IMPORTANTE: Si en algún proyecto en particular se requiriera algún acuerdo diferente para alguno de los puntos detallados en este documento, o se requiriera un punto faltante en este documento, se debe contar con la aprobación de la Secretaría de Ciudad Inteligente y Transformación Digital para llevar adelante dicho o dichos puntos en el proyecto

2. Objetivo

Este estándar tiene como objetivo definir pautas y mejores prácticas para desarrollar, implementar y administrar aplicaciones de manera efectiva, segura y escalable.

El propósito de este documento es servir como un compendio práctico y autorizado de estándares propuestos dentro del ámbito de la Municipalidad de Córdoba.

3. Alcance

Los estándares de Tecnología de Información y Comunicaciones se aplican a todas las dependencias y organismos auxiliares del Gobierno de la Municipalidad de Córdoba.

Este estándar se aplica a todo el desarrollo de software nuevo que se implemente en el ámbito de la Municipalidad de Córdoba, abarcando aplicaciones web, aplicaciones móviles, backends, servicios y cualquier otro tipo de software que se ejecute en la infraestructura dispuesta por la Municipalidad.

Se espera que todo el software desarrollado cumpla con los principios de seguridad, eficiencia, mantenibilidad y usabilidad. Este estándar busca garantizar la calidad y la coherencia en todos los proyectos de software realizados en el ámbito de la Municipalidad de Córdoba, contribuyendo así a la eficacia de los servicios ofrecidos a los ciudadanos.

4. Normativa de referencia

- Carta Orgánica Municipal de la Ciudad de Córdoba.

- Ordenanza N° 13440 del Consejo Deliberante de la Ciudad de Córdoba.
- Decreto N° 054-24 del Intendente de la Ciudad de Córdoba.

5. Autoridad

Los estándares de Tecnología de Información y Comunicaciones se publica bajo la autoridad de la Secretaría de Ciudad Inteligente y Transformación Digital del Gobierno de la Municipalidad de Córdoba. Dicha Secretaría fija las directrices y normatividad en materia de TIC, guiando el enfoque de aplicación e implementación en todo el gobierno.

6. Generalidades

El control y responsabilidad de la información de la aplicación, debe estar a cargo de un organismo perteneciente al Gobierno de la Municipalidad de Córdoba. Toda persona que utiliza o tienen acceso a información del Gobierno de la Municipalidad de Córdoba, y a otros activos asociados, debe resguardar el grado de confidencialidad e integridad de la misma, y no afectar su disponibilidad, manteniendo en todo momento protegida la información y otros activos asociados.

Se deben considerar en el diseño, desarrollo e implementación, los aspectos referentes a la seguridad informática, los que se establecerán en cada caso y en forma conjunta con el área correspondiente Secretaría de Ciudad Inteligente y Transformación Digital.

7. Requerimientos para el desarrollo de aplicaciones

7.1 Alojamiento de los sistemas

Todas las aplicaciones deben poder alojarse en la infraestructura de nube de Amazon Web Services (AWS) en la cuenta administrada por la Municipalidad de Córdoba. Este requisito se basa en la fiabilidad, escalabilidad y seguridad que ofrece AWS, así como en su amplia gama de servicios que pueden satisfacer las necesidades de cualquier aplicación.

El dimensionamiento del Hardware es responsabilidad del proveedor y debe ser especificado durante la etapa del proyecto. Es necesario comunicar a la Secretaría de Ciudad Inteligente y Transformación Digital con anticipación para disponibilizar el mismo y verificar el correcto uso.

7.2 Requerimiento de logs

Las aplicaciones deberán incluir registros (logs) en su estructura de base de datos para registrar eventos relevantes y acciones realizadas en la base de datos. Estos logs deben contener información detallada sobre operaciones como inserciones, actualizaciones y eliminaciones de datos, así como eventos importantes relacionados con la seguridad y la

integridad de los datos.

Para obtener más detalles sobre los requisitos específicos para los logs de base de datos, se recomienda revisar el documento Estándar de Bases de Datos Municipalidad de Córdoba. Este documento proporciona directrices adicionales y mejores prácticas para el diseño y mantenimiento de bases de datos en el contexto de la Municipalidad de Córdoba.

7.3 Browsers e Interface con el Usuario

7.3.1 Compatibilidad con Navegadores

Todas las aplicaciones desarrolladas deben garantizar una funcionalidad consistente y una experiencia visual coherente en todos los navegadores web comunes. Esto incluye, pero no se limita a, Google Chrome, Mozilla Firefox, Microsoft Edge y Safari.

Se debe realizar un esfuerzo para probar y asegurar que la aplicación funcione correctamente en cada uno de estos navegadores, teniendo en cuenta las diferencias en la interpretación de estándares web y el rendimiento de la interfaz de usuario.

7.3.2 Uso de Componentes y Licenciamiento

Queda prohibido el uso de componentes que requieran instalación en la computadora del usuario y que estén sujetos a licenciamiento o dependan de un sistema operativo propietario.

Todas las funcionalidades de la aplicación deben ser implementadas utilizando componentes que estén disponibles en la web y no requieran licencias adicionales para su uso. Esto garantiza la accesibilidad y la eliminación de posibles obstáculos legales relacionados con la propiedad intelectual o el costo de licencias de software.

7.4 Plataformas de desarrollo

Las plataformas de desarrollo autorizadas se se establecerán en cada caso y en forma conjunta con el área correspondiente de la Secretaría de Ciudad Inteligente y Transformación Digital.

El software usado en el desarrollo de aplicaciones, debe estar dentro del paradigma de "código abierto".

7.5 Bases de datos

Para obtener detalles sobre bases de datos autorizadas para los sistemas, los requisitos específicos para los logs de base de datos, etc., se recomienda revisar el documento Estándar de Bases de Datos.

7.6 Disponibilidad de Datos (API)

Cada aplicación debe tener una API REST accesible que exponga la información relevante de la información que administra en un formato adecuado para su extracción y uso externo. También se espera que la aplicación se integre con otras aplicaciones y utilice los datos que proporcionan para evitar redundancias innecesarias de datos almacenados.

7.6.1 Consideraciones para la Implementación y Uso de APIs

Las APIs REST (Representational State Transfer) facilitan la comunicación eficiente entre sistemas a través de internet al basarse en estándares web como HTTP. Estas ofrecen una serie de ventajas que las hacen ideales para el desarrollo de aplicaciones:

- **Sencillez:** Gracias a su enfoque en estándares web ampliamente conocidos, como HTTP y URI, las APIs REST son fáciles de entender y utilizar.
- **Flexibilidad:** Permiten la integración entre sistemas heterogéneos, ya que pueden ser consumidas por cualquier aplicación capaz de realizar solicitudes HTTP.
- **Escalabilidad:** Las APIs REST pueden manejar fácilmente un gran número de solicitudes, haciéndolas ideales para entornos con alta demanda.
- **Portabilidad:** Al utilizar formatos de datos estándar como JSON o XML, las APIs REST son independientes del lenguaje de programación o plataforma, facilitando su implementación en diferentes entornos.
- **Mantenibilidad:** La arquitectura sin estado de las APIs REST simplifica el mantenimiento y la evolución de los sistemas, ya que cada solicitud contiene toda la información necesaria para ser procesada por el servidor.

Las APIs REST desarrolladas deberán cumplir las siguientes pautas:

Diseño de Recursos: Definir recursos claramente identificables que representen entidades específicas del dominio del sistema.

Rutas y verbos HTTP: Asociar cada recurso con una URI única y utilizar los verbos correspondientes HTTP estándar (GET, POST, PUT/PATCH, DELETE) a las operaciones que se van a realizar.

Formato de Datos: Utilizar el formato de datos JSON para representar la información intercambiada entre el cliente y el servidor.

Estado de la Sesión: Mantener la comunicación sin estado (stateless), donde cada solicitud del cliente contiene toda la información necesaria para ser procesada por el servidor, sin depender de sesiones previas.

Seguridad: Implementar medidas de seguridad apropiadas, como autenticación y autorización, para proteger las rutas y restringir el acceso a recursos sensibles.

Documentación y Versionado: Documentar exhaustivamente la API, incluyendo descripciones claras de cada recurso, sus URIs, los parámetros aceptados y las respuestas esperadas. Si es necesario, implementar un sistema de versionado en la URI de la API para

permitir cambios afectar el funcionamiento actual, logrando así la compatibilidad con las versiones anteriores.

Gestión de Errores y Pruebas: Manejar errores de manera adecuada, proporcionando mensajes de error descriptivos y sugerencias para su resolución. Realizar pruebas exhaustivas de la API, incluyendo pruebas unitarias, de integración y de extremo a extremo, para garantizar su correcto funcionamiento y fiabilidad.

8. Requerimientos No Funcionales

Los requerimientos no funcionales (RNF) son restricciones de los servicios o funciones ofrecidas por el software. Incluyen restricciones de tiempo y recursos, sobre el proceso de desarrollo, estándares, etc.

Son aquellos requerimientos que no se refieren directamente a las funciones específicas del sistema, sino a las propiedades emergentes de éste como la fiabilidad, la respuesta en el tiempo y la capacidad de almacenamiento.

Muchos RNF se refieren al sistema completo y no tanto a rasgos particulares del mismo. Esto significa que muchas veces pueden resultar más críticos que los requerimientos funcionales (RF) particulares. Mientras que el incumplimiento de este último degradará el producto final, una falla en un RNF puede inutilizar el mismo.

Surgen de la necesidad del usuario, debido a las restricciones en el presupuesto, a las políticas de la organización, a la necesidad de interoperabilidad con otros sistemas de software o hardware o a factores externos como los reglamentos de seguridad, las políticas de privacidad, etcétera.

En general, los RF definen lo que un software se supone que debe hacer, mientras que los RNF definen cómo un software se supone que es.

A continuación, se detallan algunos requisitos a cumplir.

8.1 Autenticación

Las aplicaciones desarrolladas deben autenticar a los usuarios utilizando el inicio de sesión de Vedi, y también deben permitir que los usuarios cierren sesión a través de esta plataforma.

8.2 Logging

El nivel de logging de los sistemas a implementar debe ser definido de manera apropiada, considerando la naturaleza y complejidad de cada uno. Se debe establecer un nivel de logging adecuado para garantizar la captura de información relevante para el monitoreo, diagnóstico y resolución de problemas, sin comprometer el rendimiento del sistema.

8.3 Administración de Errores

La aplicación debe evitar enmascarar los mensajes de error HTTP de manera que los balanceadores y proxies puedan interpretar el estado actual de la aplicación.

En caso de que ocurra un error inesperado, no se deben mostrar características del servidor, dirección IP, ruta (path), ni cualquier otra información que pueda revelar detalles de la infraestructura subyacente. Esto garantiza la seguridad y la confidencialidad de la infraestructura tecnológica, al tiempo que permite una correcta gestión de errores por parte de los componentes de la red, facilitando la identificación y resolución de problemas.

8.4 Disponibilidad

Todas las aplicaciones desarrolladas deben garantizar una disponibilidad continua, aprovechando la infraestructura altamente disponible proporcionada por el proveedor de AWS. Se espera que las aplicaciones estén disponibles las 24 horas del día, los 7 días de la semana (7x24), sin interrupciones que afecten significativamente el acceso a los servicios.

Para cumplir con este requisito, se debe diseñar y desarrollar cada aplicación considerando las mejores prácticas de alta disponibilidad recomendadas por el proveedor de servicios en la nube. Además, se deben implementar mecanismos de monitoreo proactivo para detectar cualquier anomalía en el rendimiento o la disponibilidad de la aplicación.

8.5 Modularidad y escalabilidad

Se debe proveer escalabilidad horizontal en el sistema a desarrollar.

Para garantizar la escalabilidad y la flexibilidad de las aplicaciones, es fundamental que los distintos servicios, incluidos los servidores de aplicaciones, las bases de datos y otros servicios, estén diseñados de manera desacoplada.

El desacoplamiento de componentes proporciona flexibilidad y escalabilidad al permitir el despliegue independiente y la escalabilidad horizontal de cada parte de la aplicación. Además, facilita la gestión de la seguridad al permitir la aplicación de políticas de red y control de acceso adaptadas a cada tipo de componente.

Se debe priorizar el diseño de la arquitectura de la aplicación de manera que los componentes puedan comunicarse de manera eficiente y segura a través de la red, independientemente de su ubicación física o lógica.

8.6 Usabilidad y Experiencia de Usuario

Es esencial que todas las aplicaciones mantengan una coherencia estética que refleje el diseño gráfico integral de la Municipalidad de Córdoba, a la par que ofrezcan una experiencia de usuario óptima. Por esta razón, todos los desarrollos deben ser evaluados y aprobados por la Dirección de Sistemas de la Secretaría de Ciudad Inteligente y

Transformación Tecnológica, asegurando así una cohesión visual y una experiencia de usuario consistente en todas las plataformas digitales asociadas al gobierno municipal.

Este requisito fortalece la identidad visual de la ciudad, garantizando al mismo tiempo una experiencia unificada y satisfactoria para los usuarios.

Estética: Todas las aplicaciones de la Municipalidad de Córdoba deben tener una concordancia estética homogénea que se corresponda con la marca integral del Gobierno Municipal. Por este motivo, todos los diseños, ya sean de aplicaciones accedidas desde la intranet o desde internet, deben tener la conformidad de comunicación.

Responsive: Todas las aplicaciones de la Municipalidad de Córdoba deben cumplir con la condición de ser Responsive Web Design (RWD), de tal forma que la apariencia se adapte a diferentes dispositivos tecnológicos (tales como tablets, smartphones, portátiles, etc.).

8.7 Validación de los Datos de Entrada

Todas las pantallas de ingreso de datos deben validar la entrada del usuario en cuanto a tipo de dato, longitud y rango válido. Las validaciones deben realizarse tanto en la capa de presentación como en el servidor, sin confiar únicamente en las validaciones del cliente. Se debe presumir que los datos ingresados son incorrectos hasta que se demuestre lo contrario.

8.8 Subida de Archivos

Las aplicaciones que requieran subir archivos, ya sea que estos sean generados por la misma aplicación o cargados por usuarios finales, deben integrarse con la plataforma de Centro de Documentación Digital de la Municipalidad de Córdoba.

8.9 Entrega de Actualizaciones

El proveedor deberá proporcionar a la Municipalidad de Córdoba las entregas de las versiones desarrolladas, acompañadas de un documento de "Release Notes". Estas actualizaciones deben ser entregadas de manera oportuna y consistente con el plan de desarrollo acordado.

El documento de "Release Notes" deberá incluir información detallada sobre los cambios realizados en la versión, nuevas características agregadas, errores corregidos y cualquier otra información relevante para la implementación y el uso efectivo de la actualización por parte de la Municipalidad.

8.10 Versionado

Es obligatorio que cada producto a instalar cuente con una etiqueta de versión claramente visible, siguiendo las reglas del estándar de versionado semántico:

- La versión beta se considera una versión funcional completa. El equipo de proyecto debe justificar que se han cumplido los requisitos y expectativas.
- La versión estable se denota como 1.0.0. A partir de esta versión, se aplican las siguientes reglas:
  - 1.0.Z: Se utiliza para corregir incidencias encontradas en la versión 1.0.0.
  - 1.Y.0: Si la cifra Y se incrementa, la cifra Z se establece en cero, lo que indica la incorporación de mejoras y posiblemente correcciones de incidencias.
  - X.0.0: Esta etiqueta implica los mismos cambios que la anterior, pero también indica cambios significativos en varios aspectos, como diseño, funcionalidades, interfaz de usuario, entre otros.

8.11 Transferencia de Conocimientos

Se requerirá al desarrollador de las aplicaciones que realice la transferencia de conocimientos del proyecto a un grupo de funcionarios de la Secretaría de Ciudad Inteligente, con el objetivo de minimizar los inconvenientes. Este traspaso implicará la entrega de las versiones más recientes de la documentación funcional y de diseño relacionada con el proyecto, así como la capacitación de los funcionarios técnicos.

Dicha capacitación cubrirá aspectos clave, como la estructura del código fuente, las particularidades de compilación y funcionamiento del sistema, así como la configuración y parametrización necesarias para la implementación y mantenimiento del desarrollo en los casos en que aplique.

9. Entregables

Se detallan a continuación los entregables mínimos requeridos para un proyecto de desarrollo de software y el contenido esperado en cada uno de ellos:

Entregable	Contenido
Documento de Proyecto	• Objetivo y alcance del proyecto. • Cronograma de tareas. • Plan de entregables del proyecto e identificación de hitos.
Documento de Requerimiento	• Documento de requerimientos (funcionales y no funcionales). • Requerimientos funcionales acordados y priorizados.

021

Documento de Arquitectura	• Modelo lógico y físico de datos. • Ambientes requeridos. • Herramientas de desarrollo. • Arquitectura tecnológica (sistema operativo, software de base, motor de base de datos, etc.).
Paquetes de software	Para cada entrega acordada con el proveedor se debe presentar: • Código fuente generado en su totalidad instalado en los ambientes de Desarrollo de la Municipalidad de Córdoba. • Instalación de todos los componentes de software adicionales necesarios para el correcto funcionamiento de lo entregado. • Documento de requerimientos / funcionalidades incluidas en el paquete entregado. • Documento de control de cambios. • Transferencia de conocimiento. • Manual de operaciones e instalación. • En caso de que posea una Api, Documento de especificación de esta.
Documento Manual de Usuario	Documentación completa del software que incluya todas las funcionalidades para todos los roles y la administración de roles, permisos y seguridad.
Material de Capacitación	• Propuesta con el plan de capacitación. • Documentación que incluya la completitud de la funcionalidad a capacitar

10. Buenas Prácticas

Es deseable que durante el proceso de desarrollo de aplicaciones se sigan las siguientes buenas prácticas:

Adherencia a los Principios S.O.L.I.D.: Se recomienda tener en cuenta los principios S.O.L.I.D. al diseñar y desarrollar las aplicaciones, con el fin de mejorar la calidad y la mantenibilidad del código.

Utilización de Patrones de Diseño: Se alienta el uso de patrones de diseño apropiados en la construcción de la solución de software, para promover la escalabilidad, la reutilización y la legibilidad del código.

Implementación de Pruebas: Se deben realizar pruebas unitarias, de integración y end-to-end de manera sistemática para garantizar la funcionalidad, la interoperabilidad y la

021

robustez del sistema. Además, en casos de sistemas críticos, se recomienda realizar pruebas de estrés para evaluar la capacidad de respuesta bajo cargas extremas.

Empleo de Herramientas de Análisis de Código Estático: Se sugiere utilizar herramientas de análisis de código estático de forma regular durante el proceso de desarrollo, ya que estas herramientas contribuyen significativamente a mejorar la calidad del software al identificar posibles problemas de código, vulnerabilidades y malas prácticas de programación

ING. GUSTAVO E. SARAVIA
Subsecretario de Infraestructura
Tecnológica y Conectividad
Secretaría Ciudad Inteligente
y Transformación Digital

Secretaría de
Ciudad Inteligente y Transformación Digital

Municipalidad de Córdoba

Política General de Infraestructura Tecnológica

MUNICIPALIDAD DE CÓRDOBA

SECRETARÍA DE CIUDAD INTELIGENTE Y TRANSFORMACIÓN DIGITAL

SUBSECRETARÍA DE INFRAESTRUCTURA TECNOLÓGICA Y CONECTIVIDAD

Versión 1.0

021

Título	POLÍTICA GENERAL DE INFRAESTRUCTURA TECNOLÓGICA				
Resumen	Este documento describe la Política General de Infraestructura Tecnológica de la Municipalidad de Córdoba.				
Tipo	Política	**Versión**	1.0	**Código**	POL-002

Nivel de circulación:	Público.
Clasificación	No Confidencial. Propiedad de la Municipalidad de Córdoba.

Ciclo de Aprobación			
	Nombre	**Posición/Cargo**	**Fecha**
Revisado	Alejandro Gómez	Jefe de Infraestructura	12/07/2024
Revisado	Gustavo Saravia	Subsecretario de Infraestructura Tecnológica y Conectividad	12/07/2024
Aprobado	Ignacio Gei	Secretario de Ciudad Inteligente y Transformación Digital	16/07/2024

Registro de cambios			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	21/06/2024	Facundo N. Oliva Cúneo (Director de Ciberseguridad)	Creación del documento.

021

23 JUL 2024

Contenido

021

12 JUL 2024

1. Introducción

Una política, es una declaración de alto nivel que describe la posición de la entidad sobre un tema específico, en este caso, sobre Infraestructura Tecnológica, y que brinda lineamientos para la gestión.

La infraestructura tecnológica es el conjunto de sistemas hardware y software, junto con las personas, necesarios y necesarias para el correcto funcionamiento, la adecuada gestión y el buen uso, de los servicios brindados por la organización, ya sean servicios internos o externos, que son total o parcialmente apoyados por tecnologías de la información y las comunicaciones.

En la gestión de la Infraestructura tecnológica, se cruzan diversos ejes contingentes que tienen que ser considerados y armonizados, entre ellos:

- Por un lado, para la Municipalidad de Córdoba es importante asegurar tanto la calidad como la protección de la información y los servicios, garantizando una adecuada gestión y administración integral de su Infraestructura Tecnológica, y reconoce que la articulación de la tecnología y los procesos, así como las personas, son fundamentales para la adecuada operación de la Institución.
- Por otro lado, el desarrollo de servicios y aplicaciones sucede en un entorno tecnológico caracterizado por su diversidad y constante transformación. Los diferentes modelos ("cloud" o "en la nube", "on premise" o "en instalaciones propias", o "modelos híbridos"), las diversas plataformas (diversos sistemas operativos, servidores de aplicaciones, bases de datos, etc.), la variedad de lenguajes de desarrollo y la evolución de las tecnologías de integración e interoperabilidad, etc., ofrecen alternativas de mejoras y ventajas, que son demandadas por los desarrolladores, quienes esperan con ellas brindar mejores servicios a los usuarios.

Esta situación plantea desafíos para la gestión de la infraestructura tecnológica, en cuanto a la toma de decisiones y el riesgo de encontrarse en el futuro lidiando con un conjunto heterogéneo de sistemas y aplicaciones.

En virtud de todo lo anterior, la Municipalidad de Córdoba establece la presente Política General de Infraestructura Tecnológica, en búsqueda de la aplicación de buenas prácticas y estándares internacionales, a la vez en cumplimiento del marco normativo superior, que permitan la operatividad e interoperabilidad continua de las plataformas tecnológicas, calidad y protección de los servicios y la información, y una buena gestión y administración de la infraestructura Tecnológica, sostenible en el tiempo, garantizando su disponibilidad, integridad y confidencialidad, y mejora continua.

Una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance, sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro de la entidad. Se intenta esto en la presente, y

021

este debe ser el criterio guía para el desarrollo del marco documental que de la presente se desprenda.

2. Objetivo

Los objetivos de la presente Política General de Infraestructura Tecnológica, son:

La operatividad e interoperabilidad continua de las plataformas tecnológicas, la calidad y protección de los servicios y la información, y una buena gestión y administración de la infraestructura Tecnológica, sostenible en el tiempo, garantizando su escalabilidad y agilidad, a la ves de su disponibilidad, integridad y confidencialidad.

Formalizar consideraciones a tener en cuenta al establecer los requerimientos para el hardware y software de los centros de datos, infraestructuras de red de comunicaciones, sistemas de usuario final y servicios administrados por la Municipalidad de Córdoba.

Optimizar la relación costo beneficio de los esfuerzos económicos.

3. Ámbito de aplicación y alcance

Esta política general se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la infraestructura tecnológica de la Municipalidad de Córdoba.

Esta Política, y las normativas que de la misma deriven, alcanza y aplica a la información y a la infraestructura tecnológica de la Municipalidad de Córdoba, incluyendo a sus dependencias y organismos auxiliares.

Esta Política, y las normativas que de la misma deriven, alcanza y aplica al personal de Municipalidad de Córdoba en su conjunto (incluyendo al personal de todas sus dependencias y organismos auxiliares), como así también, a toda persona, colaborador y/o terceros que accedan y/o utilicen información y/o recursos de tecnología informática y comunicaciones de Municipalidad de Córdoba, y por ende, son responsables de contribuir al logro y mantenimiento de sus objetivos.

Los criterios establecidos en este documento serán también aplicables para los integradores que implementen todo tipo de sistemas desarrollados por terceros dentro de la infraestructura tecnológica de la Municipalidad, en cumplimiento de contratos que así lo soliciten. Estas implementaciones, deberán efectuarse respetando los criterios de arquitectura y entornos de desarrollo, homologación y producción descriptos en este documento (y/o sus derivados) de tal forma que los sistemas producto de la contratación puedan ser implementados en Centro de Datos gestionados por la Municipalidad de Córdoba.

4. Disposiciones Generales y Transitorias

Los criterios y directivas emitidos en revisiones anteriores de esta Política y los referidos en cualquier otra norma al respecto, quedan totalmente sustituidos a partir de la vigencia de la presente. Así, la presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

Este documento contiene información de uso interno, propiedad de la Municipalidad de Córdoba. Antes de utilizar alguna copia de este documento, verifique que la Versión sea igual a la informada por el responsable del mismo. Si este documento es una copia impresa, verifique la validez en el timbre de Copia Impresa Controlada. De no ser válido, destruya la copia para asegurar que no se haga de ésta un uso no previsto.

5. Normativa de referencia

Normativa superior de referencia:

- Carta Orgánica Municipal de la Ciudad de Córdoba.
- Ordenanza N° 13440 del Consejo Deliberante de la Ciudad de Córdoba.
- Decreto N° 054-24 del Intendente de la Ciudad de Córdoba.
- Leyes provinciales y nacionales en la materia, incluidas las siguientes:
  - Ley N° 11.723 "Régimen Legal de la Propiedad Intelectual".
  - Ley N° 25.506 "Ley de Firma Digital".
  - Ley N° 25.326 "Protección de los datos personales".
  - Ley N° 27.590 "Ley Mica Ortega (Grooming)".
  - Ley N° 26.388 "Delitos Informáticos y Ciberseguridad".
  - Ley N° 27.411 "Aprobación del Convenio sobre Ciberdelito del Consejo de Europa".

La presente política está alineada con la siguiente normativa interna:

- "Política General de Seguridad de la Información, Seguridad Informática y Ciberseguridad" de la Municipalidad de Córdoba.

6. Autoridad

La Política de Infraestructura Tecnológica de la Municipalidad de Córdoba, se publica bajo la autoridad de la Secretaría de Ciudad Inteligente y Transformación Digital del Gobierno de la Municipalidad de Córdoba. Dicha Secretaría fija las directrices y normatividad en materia de TIC, guiando el enfoque de aplicación e implementación en todo el gobierno municipal.

7. Contenido

En el marco de la Gestión y Administración de la Infraestructura Tecnológica de la Municipalidad de Córdoba, y en el diseño e implementación de sus sistemas hardware y software, se deben atender las siguientes consideraciones:

- Operatividad continua, calidad y protección de los servicios.
- Disponibilidad, integridad y confidencialidad de la información.
- Integración e Interoperabilidad (interna y externa) entre plataformas, sistemas y servicios.
- Escalabilidad ágil de la infraestructura tecnológica.
- Gestión y administración de calidad y sostenible en el tiempo, considerando:
    - Herramientas, servicios y recursos estándares, para gestión y soporte.
    - Un adecuado esquema que asegure la detección y diagnóstico de problemas de acuerdo a las necesidades de servicio requerida por la Municipalidad de Córdoba.
    - Entornos operativos que garanticen la disponibilidad de las aplicaciones y sistemas de información.
- Uso de plataformas de código abierto.

La información y los datos de la Municipalidad de Córdoba debe estar bajo su gestión y administración, y alojada en su infraestructura tecnológica.

Se debe optimizar la relación costo beneficio de los esfuerzos en infraestructura tecnológica.

Los requerimientos de Infraestructura Tecnológica deben estar basados en normas, estándares y buenas prácticas. Los requerimientos de Infraestructura Tecnológica se refieren a tales como los siguientes:

- Requerimientos para el análisis, diseño, desarrollo, adquisición, pruebas, despliegue, actualización, cambio o baja, de sistemas hardware y software de la infraestructura tecnológica de la Municipalidad de Córdoba (infraestructura de centros de datos, infraestructuras de red de comunicaciones, sistemas de usuario final y servicios, etc.; ya sean "on premise", o "cloud", o híbridos).
- Requerimientos para la gestión y operación de dichos sistemas.
- Requerimientos para la gestión de datos e información (gestión de la generación, almacenamiento, procesamiento, modificación, eliminación, transmisión y recepción, de datos e información.).
- Requerimientos organizacionales relacionados.

- Requerimientos de la documentación derivada de la presente.

Para ello, la Municipalidad de Córdoba define que su Política General de Infraestructura tecnológica, esté alineadas a las normas y estándares sitos en el anexo "Normas, Estándares y Buenas prácticas de referencia" (en sus versiones actualizadas), que se aplicarán según las necesidades y particularidades de la Municipalidad de Córdoba.

Esta definición también regirá para el cuerpo normativo dependiente de la presente, tales como políticas de tópicos específicos, procedimientos, estándares, informes técnicos, etc., que constituyen el marco completo de cobertura de la gestión de la infraestructura tecnológica de la Municipalidad de Córdoba.

Anexo: Normas, Estándares y Buenas prácticas de Referencia

La Municipalidad de Córdoba define que su Política General de Infraestructura tecnológica, y sus normativas derivadas, estén alineadas a las siguientes "Normas, Estándares y Buenas prácticas de referencia" (en sus versiones actualizadas), que se aplicarán según las necesidades y particularidades de la Municipalidad de Córdoba. La siguiente lista no es taxativa y se da a modo de referencia y guía:

- **ISO-IEC 27001**: Esta norma internacional permite el aseguramiento y requisitos con un programa de sensibilización, cultura, adopción y comunicación en gestión de seguridad de los datos e información, según la política de seguridad de la información.
- **ISO-IEC 27002**: Esta norma internacional proporciona una lista de objetivos de control comúnmente aceptados y controles de mejores prácticas que se utilizarán como guía de implementación al seleccionar e implementar controles para lograr la seguridad de la información.
- **ISO 20000-1**: La Organización Internacional de Estandarización (ISO), a través de las normas recogidas en ISO/IEC 20000, establece una implementación efectiva y un planteamiento estructurado para desarrollar servicios de tecnología de la información fiables en lo referente a la gestión de servicios de TI.
- **ISO 20000-9**: Guía para la aplicación de ISO/IEC 20000-1 a servicios en la nube. Se trata de una guía para implementar ISO / IEC 20000-1 en proveedores de servicios que ofrecen servicios en la nube (Cloud Services). Es aplicable a diferentes categorías de servicios en la nube, como las definidas en ISO/IEC 17788 / ITU-T Y.3500 e ISO/IEC 17789 / ITU-T Y.3502. Cubre todo tipo de servicios en la nube tales como:
  - Servicio (IaaS) – Infraestructura
  - Servicios (PaaS) – Plataformas

- Servicio (SaaS) – Software

Todos los requisitos en ISO / IEC 20000-1 pueden ser aplicables a los proveedores de servicios en la nube. La guía se presenta como un conjunto de escenarios que pueden abordar muchas de las actividades típicas de un proveedor de servicios en la nube.

- **ISO/IEC 27013: Orientación sobre la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1:** Proporcionar a las organizaciones una mejor comprensión de las características, similitudes y diferencias de ISO/IEC 27001 e ISO/IEC 20000-1 para ayudar en la planificación de un sistema de gestión integrado que cumpla con ambas Normas Internacionales. Este documento proporciona orientación sobre la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1 para organizaciones que tienen la intención de:
  a) implementar ISO/IEC 27001 cuando ISO/IEC 20000-1 ya esté implementado, o viceversa;
  b) implementar tanto ISO/IEC 27001 como ISO/IEC 20000-1 juntas;
  c) integrar los sistemas de gestión existentes basados en ISO/IEC 27001 e ISO/IEC 20000-1.

  Este documento se centra exclusivamente en la implementación integrada de un sistema de gestión de seguridad de la información (SGSI) como se especifica en ISO/IEC 27001 y un sistema de gestión de servicios (SMS) como se especifica en ISO/IEC 20000-1. En la práctica, ISO/IEC 27001 e ISO/IEC 20000-1 también pueden integrarse con otras normas de sistemas de gestión, como ISO 9001 e ISO 14001.
- **ISO/IEC 27017**: Esta norma perteneciente a la familia ISO/IEC 27000. Incluye pautas y directrices sobre los controles de seguridad de la información relacionadas con servicios en la nube.
- **ISO/IEC 27018**: Es la norma que establece criterios sobre controles y directrices con relación a medidas de protección de Información de Identificación Personal (PII), de conformidad con los principios de privacidad en la norma ISO/IEC 29100 para entornos que de trabajo con sistemas de almacenamiento público en la nube.
- **ANSI/TIA-942**: Es un estándar de calidad que especifica los requisitos para centros de datos. La topología presentada en la norma es aplicable a cualquier centro de datos de cualquier tamaño y cubre toda la infraestructura física, incluidos, entre otros requisitos: ubicación del sitio, sistema eléctrico, mecánico, seguridad contra incendios, incendios, telecomunicaciones, seguridad y entre otros.
- **ITIL**: Este marco de referencia establece buenas prácticas de tecnología, el cual recomienda desarrollar procedimientos efectivos para controlar y definir la disponibilidad, la calidad y la oportunidad de los datos e información.

- **ISO 9001:** Esta Norma Internacional especifica los requisitos para un sistema de gestión de la calidad, cuando una organización:
  d) necesita demostrar su capacidad para proporcionar regularmente productos que satisfagan los requisitos del cliente y los legales y reglamentarios aplicables, y

  e) aspira a aumentar la satisfacción del cliente a través de la aplicación eficaz del sistema, incluidos los procesos para la mejora continua del sistema y el aseguramiento de la conformidad con los requisitos del cliente y los legales y reglamentarios aplicables.

Anexo: Glosario de términos

A continuación, se da una lista (no taxativa) de definiciones de algunos términos que se utilizan y deben estar claros para dar un cumplimiento apropiado a la presente política. El glosario está alineado con la *"ISO/IEC 27000: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario"* (documento al cuál se debería consultar para un listado completo):

Activo: Es cualquier elemento que tenga valor para el organismo.

Autenticidad: Validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el/la emisor/a para evitar suplantación de identidades.

Auditabilidad: Todos los eventos de un sistema deben poder ser registrados para su control posterior.

Buen uso: Es el uso de los activos que se realiza teniendo presentes las expectativas de la Municipalidad de Córdoba, esto es:

- Evitando el mal uso o abuso de los activos.
- Cumpliendo las leyes y normativas superiores, además de las políticas, estándares, procedimientos y demás normativas internas que Municipalidad de Córdoba defina.

Confiabilidad de la Información: La información generada debe ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Es la propiedad de que toda la información y todos los recursos informáticos, estén protegidos contra uso no autorizado o revelaciones accidentales, a individuos, entidades o procesos no autorizados, acorde a la clasificación otorgada por el origen y la función de la misma. Sólo las personas calificadas y autorizadas tendrán acceso a la información requerida bajo el criterio de "la necesidad de saber".

Disponibilidad: Es la propiedad de minimizar las amenazas de interrupción del negocio haciendo a la información, servicios y recursos TIC accesibles y usables cuando una entidad autorizada lo solicite, preservando la continuidad de la operatoria normal. Por lo tanto, debe

garantizar que la información de alta criticidad sea resguardada; y que la capacidad de procesamiento sea recuperada en tiempo y forma.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Evento de seguridad: Es cualquier situación que indica:

- Una posible violación a la política de seguridad de la información.
- La falta de medidas de protección.
- Una situación previamente desconocida que puede ser relevante para la seguridad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Incidente de seguridad: Uno o más eventos de seguridad que tienen una alta probabilidad de:

- Comprometer las operaciones de Municipalidad de Córdoba.
- Amenazar la seguridad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Es la propiedad de asegurar la completitud y ausencia de errores y/o corrupción en la información y los servicios, y garantizar que la información sea exacta, completa y válida de acuerdo con los valores y las expectativas de la Municipalidad de Córdoba.

Legalidad: Cumplimiento del ordenamiento jurídico (leyes, reglamentaciones, procedimientos, etc.) al que está sujeta la Municipalidad de Córdoba, y en particular, aquel que hace a la seguridad.

Mejor Práctica: Una regla de específica o una plataforma que es aceptada, a través de la industria, al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

No repudio: Refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Propietario: Persona a la que, por su cargo y/o responsabilidad, la Municipalidad de Córdoba reconoce como responsable de una información y/o un recurso TIC y/o servicio determinado. Su nivel deberá ser consistente con la autoridad requerida para evaluar los riesgos a los que está expuesto el recurso (información, TIC y/o servicio), respetar las medidas de protección para reducirlos, o para asumir los riesgos que no desee minimizar, dentro de los rangos de riesgos aprobados. Es responsable de establecer el nivel de criticidad y confidencialidad del recurso TIC y/o servicio del que es propietario.

Protección a la duplicación: Asegura que una transacción sólo se realiza una (1) vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Recurso TIC: Recurso de tecnología informática y comunicaciones.

Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, cuando las siguientes propiedades de la información apliquen, es la preservación de la autenticidad, auditabilidad, protección a la duplicación, no repudio, legalidad y confiabilidad.

Sistema de Información. Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, clasificación, procesamiento, mantenimiento, transmisión y/o difusión de información según determinados procedimientos, tanto automatizados como manuales.

Sistema de gestión de la seguridad de la información: Es la parte del sistema de gestión general, que considera los riesgos de Municipalidad de Córdoba para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Tecnología de la Información: Se refiere al hardware y software operados por la Municipalidad de Córdoba, o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Municipalidad.

Tercero: Se refiere a personas externas a Municipalidad de Córdoba que pertenecen a alguna de las siguientes categorías:

- **Proveedor:** Se refiere a organismos prestadoras de servicios, los organismos contratistas, sub-contratistas y cualquiera que, por cuenta propia o de terceros, desarrolle trabajos para o por cuenta de la Municipalidad de Córdoba.
- **Visitante:** Es cualquier persona externa al organismo, a la cual se le autoriza de manera restringida el acceso a los recursos o instalaciones de la Municipalidad de Córdoba. Caen en esta categoría: familiares o amigos de empleados, auditores, vendedores, etc.

Usuario: Persona a la cual se le concede autorización para acceder a la información y/o utilizar servicios y/o recursos TIC de la Municipalidad de Córdoba, en el desarrollo de su tarea específica. Incluye toda persona alcanzada por la presente política general.

ING. GUSTAVO E. SARAVIA
Subsecretario de Infraestructura
Tecnológica y Conectividad
Secretaría Ciudad Inteligente
y Transformación Digital

Secretaría de
Ciudad Inteligente y
Transformación Digital

Municipalidad
de Córdoba

Política General de Seguridad de la Información, Seguridad Informática y Ciberseguridad

---

MUNICIPALIDAD DE LA CIUDAD CÓRDOBA

SECRETARÍA DE CIUDAD INTELIGENTE Y TRANSFORMACIÓN DIGITAL

SUBSECRETARÍA DE INFRAESTRUCTURA TECNOLÓGICA Y CONECTIVIDAD

Título	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD				
Resumen	Este documento describe la Política General de Seguridad de la Información, Seguridad informática y Ciberseguridad de la Municipalidad de Córdoba.				
Tipo	Política	**Versión**	1.0	**Código**	POL-001

Nivel de circulación:	Público.
Clasificación	No Confidencial. Propiedad de la Municipalidad de Córdoba.

Ciclo de Aprobación			
	Nombre	**Posición/Cargo**	**Fecha**
Revisado	Gustavo Saravia	Subsecretario de Infraestructura Tecnológica y Conectividad	12/07/2024
Aprobado	Ignacio Gei	Secretario de Ciudad Inteligente y Transformación Digital	16/07/2024

Registro de cambios			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	14/06/2024	Facundo N. Oliva Cúneo (Director de Ciberseguridad)	Creación del documento.

Contenido

1. Introducción

Una política general, es una declaración de alto nivel que describe la posición de la organización sobre un tema específico, en este caso, sobre seguridad de la información, seguridad informática y ciberseguridad.

La presente política, establece la estrategia general sobre seguridad de la información, seguridad informática y ciberseguridad. Dicta los lineamientos generales para gestionar la protección de la información, los servicios y los recursos TIC's (tecnologías informáticas y de las comunicaciones), estableciendo un marco para el análisis, diseño e implementación medidas de seguridad; y el control de la eficacia de dichas medidas, para los fines buscados.

Es importante que los principios de esta política general sea parte de la cultura organizacional. En este sentido, la presente política cuenta con el compromiso manifiesto de las máximas autoridades de la Municipalidad de Córdoba y de los y las titulares de Unidades Organizativas estratégicas, para la difusión, consolidación y cumplimiento.

Una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance, sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro de la entidad. Se intenta esto en la presente, y este debe ser el criterio guía para el desarrollo del marco documental que de la presente se desprenda.

2. Objetivo

El objetivo de la presente Política General de Seguridad de la Información, es establecer los lineamientos y directivas generales relativas a la protección de la información y activos de tecnología informática y comunicaciones de la Municipalidad de Córdoba.

Las definiciones y lineamientos presentados en esta política, establecen las bases para la implementación de controles y medidas de seguridad informática, de la información y ciberseguridad que permitirán a la Municipalidad de Córdoba minimizar los riesgos que afectan a su información y a sus activos de tecnología informática y comunicaciones, de forma tal de asegurar la seguridad, confidencialidad, integridad y disponibilidad de los mismos.

3. Ámbito de aplicación y alcance

Esta política general se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Municipalidad de Córdoba.

Esta Política, y las normativas que de la misma deriven, alcanza y aplica a la información y/o recursos de tecnología informática y comunicaciones de la Municipalidad de Córdoba, (incluyendo a la información y/o recursos de tecnología informática y

comunicaciones de todas sus dependencias y organismos auxiliares).

Esta Política, y las normativas que de la misma deriven, alcanza y aplica al personal de Municipalidad de Córdoba en su conjunto (incluyendo al personal de todas sus dependencias y organismos auxiliares), como así también, a toda persona, colaborador y/o terceros que accedan y/o utilicen información y/o recursos de tecnología informática y comunicaciones de Municipalidad de Córdoba, y por ende, son responsables de contribuir al logro y mantenimiento de sus objetivos.

4. Disposiciones Generales y Transitorias

Los criterios y directivas emitidos en revisiones anteriores de esta Política y los referidos en cualquier otra norma al respecto, quedan totalmente sustituidos a partir de la vigencia de la presente. Así, la presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

Este documento contiene información de uso interno, propiedad de la Municipalidad de Córdoba. Antes de utilizar alguna copia de este documento, verifique que la Versión sea igual a la informada por el responsable del mismo. Si este documento es una copia impresa, verifique la validez en el timbre de Copia Impresa Controlada. De no ser válido, destruya la copia para asegurar que no se haga de ésta un uso no previsto.

5. Normativa de referencia

Normativa superior de referencia:

- Carta Orgánica Municipal de la Ciudad de Córdoba.
- Ordenanza N° 13440 del Consejo Deliberante de la Ciudad de Córdoba.
- Decreto N° 054-24 del Intendente de la Ciudad de Córdoba.
- Leyes provinciales y nacionales en la materia, incluidas las siguientes:
  - Ley N° 11.723 "Régimen Legal de la Propiedad Intelectual".
  - Ley N° 25.506 "Ley de Firma Digital".
  - Ley N° 25.326 "Protección de los datos personales".
  - Ley N° 27.590 "Ley Mica Ortega (Grooming)".
  - Ley N° 26.388 "Delitos Informáticos y Ciberseguridad".
  - Ley N° 27.411 "Aprobación del Convenio sobre Ciberdelito del Consejo de Europa".

6. Autoridad

La Política General de Seguridad de la Información de la Municipalidad de Córdoba, se publica bajo la autoridad de la Secretaría de Ciudad Inteligente y Transformación Digital del Gobierno de la Municipalidad de Córdoba. Dicha Secretaría fija las directrices y normatividad en materia de TIC, guiando el enfoque de aplicación e implementación en todo el gobierno municipal.

7. Contenido

El principal objetivo de la Seguridad Informática, de la Información y la Ciberseguridad, es cumplir con los siguientes aspectos:

Confidencialidad: Asegurar que la información, los servicios y todos los recursos TIC's asociados, estén protegidos contra accesos y usos no autorizados o revelaciones accidentales, acorde a la clasificación de criticidad otorgada. Sólo las personas y servicios autorizados tendrán acceso a la información requerida bajo el criterio de "la necesidad de saber".

Integridad: Asegurar la ausencia de errores y/o corrupción en toda la información y en todos los servicios, y garantizar que la información sea exacta, completa y válida de acuerdo con los valores y las expectativas de la Municipalidad de Córdoba.

Disponibilidad: Minimizar las amenazas de interrupción de los servicios y asegurar la disponibilidad de la información, los servicios y todos los recursos TIC's asociados cada vez que se los requiera, preservando la continuidad de la operatoria normal. Por lo tanto, debe garantizar que:

- La información de alta criticidad sea resguardada y esté disponible cuando se la requiera.
- La capacidad de procesamiento se mantenga disponible y sea recuperada en tiempo y forma ante eventuales interrupciones.

7.1 Directivas Generales

Las siguientes directivas generales (que serán detalladas en políticas particulares al tópico de aplicación), regirán la implementación de la Seguridad Informática, de la Información y Ciberseguridad en la Municipalidad de Córdoba:

Política General de Seguridad de la Información: La Municipalidad de Córdoba define que su Política General de Seguridad de la Información, sus requerimientos organizacionales y toda normativa derivada, estén alineadas a la norma ***"ISO/IEC 27002: Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información"*** *(en su versión actualizada, a la fecha, 3ra edición - 2022-02),* ***"ISO/IEC 20701: Seguridad de la información, ciberseguridad y protección de la privacidad - Sistema de Gestión de Seguridad de la Información - Requerimientos"*** *(en su versión actualizada, a la fecha, 3ra edición - 2022-10),* y demás estándares de seguridad de la información de la Serie

021

ISO/IEC 27000 derivados (cada una en sus versiones actualizadas), según las necesidades y particularidades de la Municipalidad de Córdoba.

Esta definición también regirá para el cuerpo normativo dependiente de la presente, tales como estándares específicos y procedimientos apropiadamente detallados, que constituyen el marco completo de cobertura de la seguridad informática, de la información y ciberseguridad de la Municipalidad de Córdoba.

Organización de Seguridad: El modelo de gestión establecido por la Municipalidad de Córdoba para la administración de la Seguridad informática, Seguridad de la Información y Ciberseguridad, es la definición de la **Dirección de Ciberseguridad**, unidad orgánica dependiente de la "Subsecretaría Tecnológica y Conectividad" de la "Secretaría de Ciudad Inteligente y Transformación Digital", la cual a su vez reporta en forma directa a la máxima autoridad del ejecutivo Municipal. Dicha Dirección es la unidad responsable de la gestión de la seguridad de la información, seguridad informática y ciberseguridad de la Municipalidad de Córdoba.

Clasificación y Control de la Información y Gestión de Activos: La información de la Municipalidad de Córdoba, los servicios y sistemas, y todos los recursos TIC relacionados, deberán encontrarse inventariados, tener asignados un Propietario, y deberán estar clasificados según su nivel de confidencialidad y criticidad respecto de los objetivos y funciones de la Municipalidad de Córdoba que soportan.

Evaluación y administración de Riesgos: Se analizan y evaluarán los riesgos a los que están sometidos los servicios y activos TIC de la Municipalidad de Córdoba. La unidad orgánica responsable de la Seguridad Informática, de la Información y Ciberseguridad, en conjunto con el Propietario del recurso TIC, establecerán los riesgos que pueden afectar a dicho recurso, las implicancias de su exposición, modificación o acceso no autorizado y cuáles son las medidas de protección que se deberán implementar de acuerdo con el análisis de riesgo efectuado.

Competencia del personal en materia de seguridad informática, de la información y ciberseguridad: Toda persona alcanzada por la presente política, deberá ser informada desde el momento de su ingreso a la Municipalidad de Córdoba, de las responsabilidades y derechos en materia de uso y protección de los activos (la información, los servicios y sistemas, y los recursos TIC's) de la organización. Se capacitará con y para el fin de crear conciencia acerca de la importancia que adquiere este aspecto. Se realizará un seguimiento del uso que se realiza de los activos para impedir daños e interferencias y evitar interrupciones de las actividades y servicios.

Seguridad Física y de Entorno: Se protegerán adecuadamente todos los recursos TIC de la organización y las áreas e instalaciones informáticas donde estos residen dentro de la organización, contra accesos no autorizados y daño intencional o no intencional, implementando medidas de protección acorde con la clasificación de criticidad, confidencialidad y riesgo otorgada a cada recurso.

Administración de Equipamiento, Operaciones y Comunicaciones: Se deben realizar y administrar controles de seguridad técnica en los sistemas TIC's, de forma de asegurar la disponibilidad de los equipamientos, la integridad de los servicios y procesos operativos y la seguridad en las comunicaciones, para garantizar un correcto procesamiento de la información y resguardar sus propiedades de confidencialidad, integridad y/o disponibilidad y eventualmente demás propiedades de seguridad requeridas de la misma. Todas las comunicaciones electrónicas con el exterior deberán ser protegidas, acorde con la clasificación de criticidad, confidencialidad y riesgo otorgada a la información cursada. La serie de normas de seguridad informática, de la información y ciberseguridad, son referencias validadas para el desarrollo de este punto, incluida, por ejemplo, la "ISO/IEC 27032 Ciberseguridad: Directrices para la seguridad en Internet".

Seguridad de la información para el uso de servicios en la nube: Los procesos de adquisición, uso, gestión y salida de servicios en la nube se establecerán de acuerdo con los requisitos de seguridad informática, de la información y ciberseguridad de la organización, alineados con la norma **ISO/IEC 27017:** ***Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube***, que incluye pautas y directrices sobre los controles de seguridad de la información relacionadas con servicios en la nube.

Controles de Acceso: Se deben considerar y establecer restricciones de acceso a las redes, los sistemas, las aplicaciones, los servicios y los datos, etc. El acceso a los activos deberá ser restringido de acuerdo con los requerimientos de control establecidos por sus Propietarios y bajo el criterio de "la necesidad de saber". Dicho acceso se asegurará a través de procesos de autenticación, autorización, monitoreo y posterior auditoría.

Desarrollo y Mantenimiento de Sistemas: Los principios de seguridad informática y de la información, deberán ser incorporados a los sistemas aplicativos en todo el ciclo de vida de los mismos, incluyendo los procesos de desarrollo, prueba, mantenimiento y puesta en producción de los sistemas aplicativos. Se deberán prevenir pérdidas, modificaciones o uso inadecuado de los datos, proyectos y sistemas aplicativos de la Municipalidad de Córdoba. La serie de estándares ISO/IEC 27034 (alineado a la ISO/IEC 27002) es una referencia. La serie consta de varios estándares, que profundizan en el área de tecnología de la información, técnicas de seguridad y seguridad de la aplicación, y tienen objetivo garantizar que las aplicaciones aseguren el nivel de seguridad requerido para el apoyo del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización, abordando adecuadamente muchos riesgos de seguridad.

Administración de la Continuidad de TI: Se deberán desarrollar, mantener actualizados y ser sometidos a pruebas periódicas, los planes de recuperación tecnológica para los recursos TIC esenciales, de forma tal de poder anticiparse y eventualmente responder a eventos no deseados que impacten de manera negativa sobre los procesos de negocio críticos para la Municipalidad de Córdoba. La norma "ISO/IEC 27031 Tecnología de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de la

021

información y las comunicaciones para la continuidad del negocio" es una referencia para este punto. La norma ISO 22301 es otra referencia validada para este punto. Define los requisitos que deben cumplir los "Sistemas de gestión de la continuidad del negocio" (BCMS, de Business Continuity Management Systems) para garantizar que una organización pueda continuar operando durante y después de situaciones de crisis, como desastres naturales, ciberataques, pandemias, conflictos armados o cualquier otro evento que pueda interrumpir sus actividades.

Conformidad con Leyes, Regulaciones y Normas Internas: Se deberá garantizar que la utilización de los activos (información, sistemas, servicios, recursos TIC, etc.) no provoquen infracciones o violaciones de leyes, regulaciones, ni de las obligaciones establecidas por estatutos, normas, reglamentos o contratos vigentes en cada ámbito de actuación. Asimismo, se deberá evaluar y asegurar el cumplimiento de las normas internas (políticas, estándares, procedimientos) relativos a la seguridad informática y de la información.

Definición de Roles y Responsabilidades: La implementación satisfactoria de la Política General de Seguridad de la Información, y de las medidas que de ella se desprendan, requiere la plena cooperación y la asistencia de todas las personas alcanzadas por la presente política general. Es imperativo, por lo tanto, que todo el personal sea consciente de, y opere de acuerdo con, los requisitos de seguridad aquí detallados.

Se establecerá un **comité se seguridad de la información, seguridad informática y ciberseguridad**, integrado por representantes de distintas unidades, no solamente técnicas, cuyo role es retroalimentar, asesorar y participar en la toma de decisiones en cuestiones relativas a la presente política, en coordinación con la unidad responsable de su ejecución.

Anexo: Glosario de términos

A continuación, se da una lista (no taxativa) de definiciones de algunos términos que se utilizan y deben estar claros para dar un cumplimiento apropiado a la presente política. El glosario está alineado con la ***"ISO/IEC 27000: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario"*** (norma a la cuál debería consultarse por glosario):

Activo: Es cualquier elemento que tenga valor para el organismo.

Autenticidad: Validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el/la emisor/a para evitar suplantación de identidades.

Auditabilidad: Todos los eventos de un sistema deben poder ser registrados para su control posterior.

Buen uso: Es el uso de los activos que se realiza teniendo presentes las expectativas de la Municipalidad de Córdoba, esto es:

- Evitando el mal uso o abuso de los activos.

- Cumpliendo las leyes y normativas superiores, además de las políticas, estándares, procedimientos y demás normativas internas que Municipalidad de Córdoba defina.

Confiabilidad de la Información: La información generada debe ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Es la propiedad de que toda la información y todos los recursos informáticos, estén protegidos contra uso no autorizado o revelaciones accidentales, a individuos, entidades o procesos no autorizados, acorde a la clasificación otorgada por el origen y la función de la misma. Sólo las personas calificadas y autorizadas tendrán acceso a la información requerida bajo el criterio de "la necesidad de saber".

Dirección de Ciberseguridad: Unidad orgánica de la Subsecretaría de Infraestructura Tecnológica y Conectividad, dependiente de la Secretaría de Ciudad Inteligente y Transformación Digital. Es la unidad responsable de la administración de la seguridad de la información, seguridad informática y ciberseguridad de la Municipalidad de Córdoba.

Disponibilidad: Es la propiedad de minimizar las amenazas de interrupción del negocio haciendo a la información, servicios y recursos TIC accesibles y usables cuando una entidad autorizada lo solicite, preservando la continuidad de la operatoria normal. Por lo tanto, debe garantizar que la información de alta criticidad sea resguardada; y que la capacidad de procesamiento sea recuperada en tiempo y forma.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Evento de seguridad: Es cualquier situación que indica:

- Una posible violación a la política de seguridad de la información.
- La falta de medidas de protección.
- Una situación previamente desconocida que puede ser relevante para la seguridad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Incidente de seguridad: Uno o más eventos de seguridad que tienen una alta probabilidad de:

- Comprometer las operaciones de Municipalidad de Córdoba.
- Amenazar la seguridad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas,

narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Es la propiedad de asegurar la completitud y ausencia de errores y/o corrupción en la información y los servicios, y garantizar que la información sea exacta, completa y válida de acuerdo con los valores y las expectativas de la Municipalidad de Córdoba.

Legalidad: Cumplimiento del ordenamiento jurídico (leyes, reglamentaciones, procedimientos, etc.) al que está sujeta la Municipalidad de Córdoba, y en particular, aquel que hace a la seguridad.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria, al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

No repudio: Refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Propietario: Persona a la que, por su cargo y/o responsabilidad, la Municipalidad de Córdoba reconoce como responsable de una información y/o un recurso TIC y/o servicio determinado. Su nivel deberá ser consistente con la autoridad requerida para evaluar los riesgos a los que está expuesto el recurso (información, TIC y/o servicio), respetar las medidas de protección para reducirlos, o para asumir los riesgos que no desee minimizar, dentro de los rangos de riesgos aprobados. Es responsable de establecer el nivel de criticidad y confidencialidad del recurso TIC y/o servicio del que es propietario.

Protección a la duplicación: Asegura que una transacción sólo se realiza una (1) vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

021

Recurso TIC: Recurso de tecnología informática y comunicaciones.

Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, cuando las siguientes propiedades de la información apliquen, es la preservación de la autenticidad, auditabilidad, protección a la duplicación, no repudio, legalidad y confiabilidad.

Sistema de Información. Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, clasificación, procesamiento, mantenimiento, transmisión y/o difusión de información según determinados procedimientos, tanto automatizados como manuales.

Sistema de gestión de la seguridad de la información: Es la parte del sistema de gestión general, que considera los riesgos de Municipalidad de Córdoba para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Tecnología de la Información: Se refiere al hardware y software operados por la Municipalidad de Córdoba, o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Municipalidad.

Tercero: Se refiere a personas externas a Municipalidad de Córdoba que pertenecen a alguna de las siguientes categorías:

- **Proveedor:** Se refiere a organismos prestadoras de servicios, los organismos contratistas, sub-contratistas y cualquiera que, por cuenta propia o de terceros, desarrolle trabajos para o por cuenta de la Municipalidad de Córdoba.
- **Visitante:** Es cualquier persona externa al organismo, a la cual se le autoriza de manera restringida el acceso a los recursos o instalaciones de la Municipalidad de Córdoba. Caen en esta categoría: familiares o amigos de empleados, auditores, vendedores, etc.

Usuario: Persona a la cual se le concede autorización para acceder a la información y/o utilizar servicios y/o recursos TIC de la Municipalidad de Córdoba, en el desarrollo de su tarea específica. Incluye toda persona alcanzada por la presente política general.

ING. GUSTAVO E. SARAVIA
Subsecretario de Infraestructura
Tecnológica y Conectividad
Secretaría Ciudad Inteligente
y Transformación Digital

Estándar de Telecomunicaciones

MUNICIPALIDAD DE CÓRDOBA

SECRETARÍA DE CIUDAD INTELIGENTE Y TRANSFORMACIÓN DIGITAL

SUBSECRETARÍA DE INFRAESTRUCTURA TECNOLÓGICA Y CONECTIVIDAD

Título	ESTÁNDAR DE DESARROLLO DE TELECOMUNICACIONES				
Resumen	Este documento describe el estándar para la adquisición e implementación de sistemas y subsistemas de Telecomunicaciones de la Municipalidad de Córdoba.				
Tipo	Estándar	**Versión**	1.0	**Código**	EST-003

Nivel de circulación:	Público.
Clasificación	No Confidencial. Propiedad de la Municipalidad de Córdoba.

Ciclo de Aprobación			
	Nombre	**Posición/Cargo**	**Fecha**
Revisado	Gustavo Saravia	Subsecretario de Infraestructura Tecnológica y Conectividad	29/07/2024
Aprobado	Ignacio Gei	Secretario de Ciudad Inteligente y Transformación Digital	30/07/2024

Registro de cambios			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	26/07/2024	Hugo Sanguinetti (Dir. Gral. de Telecomunicaciones), Facundo N. Oliva Cúneo (Dir. de Ciberseguridad)	Creación del documento.

Contenido

1. Introducción

El presente documento establece un estándar técnico para la adquisición o desarrollo de sistemas y subsistemas de Telecomunicaciones en el ámbito de la Municipalidad de Córdoba.

Un estándar (como lo define la ISO) "son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito". Ayudan a aclarar, guiar y controlar los procesos y actividades, y a crear un lenguaje común con el que los distintos actores (autoridades, personal técnico y usuarios internos, proveedores y ciudadanos en general) puede comunicarse claramente acerca de los necesidades, problemas y servicios relacionados o soportados por tecnologías de la información y comunicaciones (TIC's).

IMPORTANTE: Si en algún proyecto en particular se requiriera algún acuerdo diferente para alguno de los puntos detallados en este documento, o se requiriera un punto no incluido en este documento, se debe contar con la aprobación de la Secretaría de Ciudad Inteligente y Transformación Digital para llevar adelante dicho o dichos puntos en el proyecto.

2. Objetivo

Este estándar tiene como objetivo general definir pautas y mejores prácticas para la adquisición, diseño, desarrollo, implementación o administración, de sistemas de telecomunicaciones, en particular, equipos de telecomunicaciones y sistemas de cableados estructurados, de manera efectiva, segura y escalable.

El propósito de este documento es servir como un compendio práctico y autorizado de estándares propuestos dentro del ámbito de la Municipalidad de Córdoba. Entre los objetivos particulares, se tienen:

- Optimizar el uso y aprovechamiento de los recursos y medio de comunicación, reduciendo los costos de insumos y mantenimiento.
- Establecer una red de transporte de datos moderna y acorde con las normas establecidas por la Dirección General de Telecomunicaciones.
- Acercar a los ciudadanos sistemas modernos de captura de información.

3. Alcance

Los estándares de Tecnología de Información y Comunicaciones se aplican a todas las dependencias y organismos auxiliares del Gobierno de la Municipalidad de Córdoba.

Este estándar se aplica a toda adquisición, diseño, desarrollo, implementación o administración, de todo sistema de telecomunicaciones en el ámbito de la Municipalidad de

Córdoba.

Se espera que todo sistema de telecomunicaciones cumpla con los principios de seguridad, eficiencia, mantenibilidad y usabilidad. Este estándar busca garantizar la calidad y la coherencia en todos los proyectos realizados en el ámbito de la Municipalidad de Córdoba, contribuyendo así a la eficacia de los servicios ofrecidos a los ciudadanos.

Este documento proporciona el criterio mínimo de rendimiento de los elementos que comprenden un sistema de cableado estructurado completo y el criterio mínimo de rendimiento de equipos de comunicaciones, como así también las características técnicas, consideraciones generales adquisición, diseño, desarrollo, implementación y administración, de todo nuevo sistema de telecomunicaciones.

4. Normativa superior de referencia

- Carta Orgánica Municipal de la Ciudad de Córdoba.
- Ordenanza N° 13440 del Consejo Deliberante de la Ciudad de Córdoba.
- Decreto N° 054-24 del Intendente de la Ciudad de Córdoba.
- Política General de Seguridad de la Información, Seguridad informática y Ciberseguridad de la Municipalidad de Córdoba.
- Política General de Infraestructura Tecnológica de la Municipalidad de Córdoba.

5. Normas y estándares técnicos de referencia

En la aplicación de este estándar, se deben tener en cuenta las recomendaciones dadas en las norma y estándares técnicos aceptados por la industria. A continuación, se listan normas y estándares técnicos de referencia (los que tendrán que aplicarse en sus versiones actualizadas):

- ISO/IEC 11801 "Generic cabling for customer premises" (Cableado genérico para instalaciones de clientes).
- ANSI/TIA/EIA-568-A Commercial Building Telecommunications Cabling Standard (Estándar de cableado de telecomunicaciones para edificios comerciales).
- ANSI/TIA/EIA-568-A-5 Transmission Performance Specification for 4 Pair 100 ohm (100 MHz) Category 5e Cabling (Especificación de rendimiento de transmisión para cableado de categoría 5e de 4 pares y 100 ohm (100 MHz)) y sus grupos y trabajos asociados.
- ANSI/TIA/EIA SP-4195 Proposed Addendum No. 5 to TIA/EIA-568-A Additional Transmission Performance Specifications for 4-Pair 100 Ohm Enhanced Category 5 Cabling (Anexo propuesto N°5 para TIA/EIA-568-A Especificaciones de rendimiento de transmisión adicionales para cableado de categoría 5 mejorado de 4 pares y 100

ohmios).

- EIA/TIA-568-B Commercial Building Telecommunications Wiring Standard (Estándar de cableado de telecomunicaciones para edificios comerciales) y sus grupos y trabajos asociados.
- TIA/EIA-568-B.2-1 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components – Addendum 1 – Transmission Performance Specifications for 4- Pair 100 ohm (250 MHz) Category 6 Cabling (Estándar de cableado de telecomunicaciones para edificios comerciales, Parte 2: Componentes de cableado de par trenzado balanceado – Anexo 1 – Especificaciones de rendimiento de transmisión para cableado de categoría 6 de 4 pares y 100 ohmios (250 MHz)).
- TIA/EIA-568-B.3-1 Optical Fiber Cabling Components Standard – Addendum 1 – Additional Transmission Performance Specifications for 50/125 µm Optical Fiber Cables (Estándar de componentes de cableado de fibra óptica – Anexo 1 – Especificaciones adicionales de rendimiento de transmisión para cables de fibra óptica de 50/125 µm).
- EIA/TIA-568-C Commercial Building Telecommunications Wiring Standard (Estándar de cableado de telecomunicaciones para edificios comerciales) y sus grupos y trabajos asociados.
- ANSI/TIA/EIA 568-C.2: Balanced Twisted-Pair Cabling Components (Componentes del Cableado de Par Trenzado Balanceado).
- ANSI/TIA/EIA-568-C.3: Optical Fiber Cabling Components Standard (Estándar de Componentes de Cableado de Fibra Óptica).
- ANSI/EIA/TIA-569 Commercial Building Standard for Telecommunications Pathways and Spaces (Estándar de edificios comerciales para vías y espacios de telecomunicaciones).
- ANSI/EIA/TIA-606 Administration Standard for the Telecommunications Infrastructure of Commercial Buildings (Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales).
- ANSI/TIA/EIA-607 Commercial Building Grounding and Bonding Requirements for Telecommunications (Requisitos de Grounding (conexión a tierra) y Bonding (unión de partes conductoras) de edificios comerciales para telecomunicaciones).
- Building Industries Consulting Services International (BICSI) Telecommunications Distribution Methods Manual (TDMM).
- IEEE802.3AK-2004, Physical Layer and Management Parameters for 10Gb/s Operation, Type 10GBASE-CX4 (Capa física y Parámetros de gestión para funcionamiento a 10 Gb/s, tipo 10GBASE-CX4).

- TSB-155, Cabling performance and field test requirements for the 10GBASE-Tan application (Requerimientos de rendimiento y pruebas de campo del cableado para la aplicación de 10GBASE-Tan).
- IEEE802.3AN-2006, Amendment 1, Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-T (IEEE802.3 10GBASE_Tan), y TIA "Technical System Bulletin 155" (Enmienda 1, Capa física y Parámetros de gestión para funcionamiento a 10 Gb/s, tipo 10GBASE-T (IEEE 802.3 10GBASE Tan), y TIA "Boletín técnico del sistema 155")
- Norma ANSI/TIA-942, Telecommunications Infrastructure Standard for Data Centers (Estándar de infraestructura de telecomunicaciones para Centros de Datos).

6. Autoridad

Los estándares de Tecnología de Información y Comunicaciones se publica bajo la autoridad de la Secretaría de Ciudad Inteligente y Transformación Digital del Gobierno de la Municipalidad de Córdoba. Dicha Secretaría fija las directrices y normatividad en materia de TIC, guiando el enfoque de aplicación e implementación en todo el gobierno municipal.

7. Generalidades

Generalidades en relación a la adquisición de elementos y equipamiento de telecomunicaciones:

- Solamente se deben tener en cuenta bienes de marcas y de fábricas de reconocida trayectoria en el mercado.
- Los elementos y equipamientos a adquirir, deben ser nuevos, sin uso, originales de fábrica y su fabricación no deberá encontrarse discontinuada (nuevos y sin uso, significa que la Municipalidad de Córdoba será la primera usuaria de los equipos desde que estos salieron de la fábrica).
- Los elementos y equipamientos a adquirir se deben proveer con todos los cables necesarios para las interconexiones de los equipos.
- Todos los equipos deben operar con una alimentación 220[Vca] – 50[Hz], monofásico tipo estándar F+N+T de tres patas planas, con polaridad y tierra lateral, con fuente incorporada a la unidad de 220/110[V] (sin transformador externo). No se aceptan adaptadores para la conexión de los equipos a la red eléctrica.
- Los elementos y equipamientos a adquirir se deben proveer con los folletos técnicos.

Generalidades en relación a la Garantía de buen funcionamiento en la adquisición de elementos y equipamiento de telecomunicaciones:

- El equipamiento debe estar amparado por una garantía de buen funcionamiento por el término correspondiente descripto en las especificaciones técnicas, todos a partir de la recepción de los mismos (entendiéndose por "recepción" no su simple entrega, sino instalados y funcionando debiendo extenderse la correspondiente constancia con indicación de lugar, fecha y firma del funcionario receptor), con atención en el lugar de instalación, incluyendo repuestos, traslados y mano de obra.
- La garantía de funcionamiento y el mantenimiento correctivo debe ser integral, es decir, que debe comprender el servicio de reparación con provisión de repuestos originales y/o cambio de las partes que sean necesarias sin cargo alguno para la Municipalidad de Córdoba.
- El proveedor debe garantizar que el servicio técnico sea brindado por personal especializado de la empresa fabricante de los productos ofrecidos, o en su defecto, por su propio plantel especializado, el que deberá estar debidamente autorizado por los fabricantes de los productos ofrecidos.
- La garantía debe ser a partir de la fecha de aprobación del funcionamiento satisfactorio, con atención en el lugar de instalación e incluyendo repuestos, traslados y mano de obra. En el caso que el fabricante o distribuidor autorizado no cubra el período de garantía solicitado, la misma se debe cubrir con certificados de extensión de garantía avalados por escrito por el fabricante.

Generalidades en relación a la Garantía de Obsolescencia en la adquisición de elementos y equipamiento de telecomunicaciones:

- El proveedor debe garantizar que los equipos entregados a la Municipalidad de Córdoba sean de última generación y que no se encuentren en proceso de discontinuación.

Generalidades en relación al Soporte Técnico en la adquisición de elementos y equipamiento de telecomunicaciones:

- La relación para el cumplimiento de la garantía debe ser directamente entre el representante del Proveedor y la Municipalidad de Córdoba.
- Los servicios de reparación y mantenimiento deben ser llevados a cabo en las fechas y horarios que las partes acuerden mutuamente.
- Cuando la magnitud de la avería requiera el traslado del equipamiento para su reparación, el mismo debe ser por cuenta y responsabilidad del proveedor y no generará ningún costo adicional a la Municipalidad de Córdoba.
- Se debe presentar toda la información que sea necesaria para evaluar y comprobar si el proveedor se encuentra en condiciones de brindar el servicio ofrecido.

Generalidades en relación al diseño, desarrollo e implementación de sistemas de telecomunicaciones:

Se deben considerar en el diseño, desarrollo e implementación, los aspectos referentes a la seguridad informática, los que se establecerán en cada caso y en forma conjunta con el área correspondiente Secretaría de Ciudad Inteligente y Transformación Digital.

8. Sistema de Cableados Estructurados

Este apartado, contiene referencias a requerimientos y especificaciones técnicas, para el diseño, desarrollo e implementación de sistemas de cableado estructurado.

8.1 Requerimientos generales para sistemas de Cableado Estructurado

El cableado de redes de datos debe ser realizado según el concepto de "cableado estructurado".

El cableado estructurado debe ser apto para la provisión de servicios de datos, telefonía y video.

Los trabajos de cableado estructurado deben ser completos conformes a su fin, es decir:

- Aun cuando no se mencionen explícitamente en los requerimientos, pliegos o planos, deben considerarse incluidos todos los elementos, materiales, accesorios, insumos, etc., y todos los trabajos y roles (dirección técnica, mano de obra, etc.), necesarios para el cumplimiento del trabajo y el correcto funcionamiento.
- Deben considerarse las certificaciones del trabajo realizado.
- Debe considerarse la Capacitación para técnicos y operadores para la puesta en servicio completa del cableado estructurado y/o equipamiento.
- Cuando las obras a realizar debieran ser unidas o pudieran afectar en cualquier forma obras existentes, los trabajos necesarios al efecto, deben estar considerados, y a cargo del proveedor, y se considerarán comprendidos sin excepción en su propuesta.
- El proveedor es el único responsable de los daños causados a personas y/o propiedades durante la ejecución de los trabajos de instalación y puesta en servicio. El proveedor debe tomar todas las precauciones necesarias a fin de evitar accidentes personales o daños a las propiedades, así pudieran provenir dichos accidentes o daños de maniobras en las tareas, de la acción de los elementos o demás causas eventuales. El proveedor deberá reparar todas las roturas que se originen a causa de las obras, con materiales iguales en tipo, textura, apariencia y calidad no debiéndose notar la zona que fuera afectada. En el caso de que la terminación existente fuera pintada, se repintará todo el paño, de acuerdo a las reglas del buen arte a fin de igualar tonalidades.

La topología adoptada en la red de datos de área local (LAN) debe ser "Topología en Estrella", usando como centro de la misma el rack principal o la sala de Distribución Principal

correspondiente al sector. Esta ubicación es definida por la Dirección General de Telecomunicaciones.

A este rack o sala principal, se conectarán todos los racks secundarios y/o salas de Distribución que se instalen dentro del edificio.

Para la instalación de cualquier rack, sea principal o secundario, se deben contemplar los siguientes requerimientos:

- Deben estar alejados del alcance de las personas y de elementos que generen riesgos.
- No deben ser instalados encima de escritorios ni en alguna otra ubicación donde exista paso de personas.
- Deben estar alejados de las ventanas, pasos de aire, polvillo y cualquier fuente o abertura que provoque degradación del mismo.
- Deben estar instalados en ambientes sin humedad.
- Deben estar alejados de equipos eléctricos, fuentes de calor, motores, ascensores, etc.
- Sus características y ubicación respetarán las pautas de seguridad que determine el lugar de su ubicación.

Cuando la obra sea realizada por un tercero, la Dirección General de Telecomunicaciones debe designar un representante técnico que realizará el control y supervisión técnica de la obra para que el proveedor respete el presente estándar de especificaciones técnicas.

Además, en el caso de que sea necesario a criterio de la Dirección General de Telecomunicaciones de la Municipalidad de Córdoba, el personal de dicha Dirección acompañará al personal de la empresa proveedora a realizar los relevamientos correspondientes para determinar el listado de materiales necesarios para cableado y la mano de obra requerida. El listado de materiales deberá ser aprobado por la mencionada Dirección.

8.2 Presentación de propuesta de proyecto para Sistemas de Cableado Estructurado

Con la propuesta de un sistema de cableado estructurado, se debe presentar un plan de trabajo detallado, que permita efectuar un seguimiento eficiente de la ejecución de los mismos.

El plan de trabajo debe incluir la descripción técnica detallada de la solución propuesta, incluyendo indicación sobre planos a escala de la dependencia, de los siguientes puntos:

- Distribución del cableado vertical y horizontal, es decir, traza de las canalizaciones principales del cableado de vertical y de Backbones, y de cableado horizontal o de Distribución.

- Puestos de trabajos nuevos o a refuncionalizar, indicando en forma diferenciada en cada puesto, las bocas de datos y de telefonía, ya que, para ambos servicios, datos y telefonía, el sistema debe ser mediante cableado estructurado
- Ubicación de los racks principales y/o cuarto de racks principales, y ubicación de racks secundarios.

El plan de trabajo debe incluir:

- Listado de materiales requeridos para el sistema de cableado estructurado solicitado, indicando cantidad de elementos consumibles y elementos de red, discriminando los correspondientes a la red de datos y de telefonía.
- Cronograma de tareas, indicando fecha de finalización de la obra.

Todo trabajo de cableado estructurado debe cumplir los siguientes requerimientos, los cuáles se deben incluir en el plan de trabajo:

- Provisión de los cables para el cableado de la red de telecomunicaciones.
- Provisión e instalación de las cajas de conexión, conectores de telecomunicaciones en la cantidad de puestos indicadas según requerimientos.
- Provisión e instalación de todos los elementos de conectividad de los gabinetes de comunicaciones y/o salas de racks de comunicaciones.
- Provisión e instalación de gabinetes de comunicaciones (racks) para el cableado estructurado vertical y horizontal.
- Conectorizado de todas las bocas de red en los puestos de trabajo, con la provisión de rosetas y JACK RJ-45 y de los paneles de cruzada dentro de los gabinetes de comunicaciones.
- Certificación de todas las bocas según el estándar EIA/TIA -568A.

8.3 Subsistema Cableado estructurado en racks

Dentro de los racks principales y de cada rack secundario, los cables del cableado horizontal y vertical (o backbone's) terminarán en patch panell Cat5e de una unidad para montaje en bastidor de 19".

Los enlaces entre el rack principal y los racks secundarios, se deben conectar a los últimos puertos del patch panel. Por ejemplo, si el patch panell es de 24 puertos, el enlace se conectará en el puerto 24; si el patch panell es de 48 puertos, el enlace se conectará en el puerto 48.

Cross Connect (Conexiones cruzadas): Las cruzadas para los circuitos de datos se realizarán mediante Patch Cords, desde los Patch Panels Enhanced Category 5 del tendido horizontal de datos, hacia el Hardware de Networking dentro del mismo rack o hacia bastidores contiguos.

Se deben prever todos los patch cord necesarios para las conexiones de cruzadas dentro de los racks (principales y secundarios). Dentro del rack se utilizarán patch cords Enhanced Category 5 de 0,6 m para realizar la conexión entre los patch panels y el hardware de red (Switch). Los patch cords deben ser ensamblados y testeados en fábrica por el fabricante del sistema de cableado.

Instalación del cableado en el rack: El hardware de terminación de cobre y hardware de management (manejo) de cables, se instalará de la siguiente manera:

- Se acomodarán y se terminarán los cables de acuerdo con las recomendaciones hechas en la TIA/EIA-568-A, las recomendaciones del fabricante y/o buenas artes de la industria.
- El destrenzado de los pares de los cables Cat5e en el área de terminación será el mínimo posible y en ningún caso será superior a media pulgada (12,7 mm).
- Los radios de curvatura de los cables en el área de realización de la terminación no serán menores a 4 veces el diámetro externo del cable.
- La vaina del cable se mantendrá tan cerca como sea posible del punto de terminación.
- Los mazos de cables se precintarán y acomodarán en forma prolija a sus respectivos patch panels. Cada patch panel será alimentado por un mazo de cables individualmente separado, acomodado y precintado hasta el punto de entrada al rack. No debe olvidarse precintar cada uno de los cables a la barra de sujeción posterior.
- Cada cable se etiquetará claramente en la vaina, detrás del patch panel en una ubicación que pueda verse sin quitar los precintos de sujeción del mazo. No se aceptarán cables cuya identificación no sea claramente visible o se encuentre oculta dentro del mazo de cables.

El hardware de terminación de fibra óptica se instalará de la manera siguiente:

- El exceso de cable de fibra óptica se enrollará en forma prolija en las anillas organizadoras que se encuentran dentro de los Patch Panel deslizables de fibra óptica.
- Se tendrá presente que al alojar el rollo del cable no se deben exceder los radios de curvatura mínimos recomendados por el fabricante.
- Cada cable se precintará en forma individual dentro del hardware de terminación respectivo, mediante medios mecánicos. El o los "strength members" de los cables de fibra óptica, se sujetarán a los accesorios internos del hardware de terminación dispuestos internamente para tal fin.
- Cada cable de fibra óptica se despojará de su vaina al entrar en el hardware de terminación y se ruteará cada una de las fibras en forma individual hacia los acopladores ópticos.

- Cada cable se etiquetará claramente a la entrada del hardware de terminación. No se aceptarán cables que se hallen etiquetados dentro de los mazos y sus identificaciones no sean claramente visibles.
- Los protectores de polvo se dejarán instalados en todo momento en los conectores y acopladores, a menos que se hallen físicamente conectados.

Jacks Modulares: Especificaciones de referencia:

- Tipo RJ45. Se conectarán de acuerdo a la asignación de colores T568A/T568B.
- Housing de óxido de polifenileno, valorado 94V-0, con terminaciones usando un conector estilo 110 para montaje en circuito impreso (realizado en policarbonato valorado 94V-0), con etiqueta de codificación de colores para T568A y T568B.
- El conector tipo 110 debe aceptar conductores sólidos de 22-24 AWG, con un diámetro de aislación máxima de 0.050 pulgadas. Los contactos del jack modular deben estar bañados con un mínimo de 50 micropulgadas de oro en el área del contacto y un mínimo de 150 micropulgadas de estaño en el área de la soldadura, encima de un bajo baño mínimo de 50 micropulgadas de níquel.
- Los jacks modulares deben ser Compatibles con un panel de montaje estándar (espesor entre 0.058" - 0.063" y abertura de 0.790" X 0.582"). Los jacks modulares serán listados bajo el número UL E81956.
- Los jacks modulares Enhanced Category 5 deberán ser non-keyed, de 4-pares y deberán cumplir los requerimientos standards de performance EIA/TIA Category 5.
- Los jacks modulares deberán cumplir con los requerimientos de performance propuestos en la TIA/EIA-SP-4195, "Additional Transmission Performance Specifications for 4-Pair 100 Ohm Enhanced Category 5 Cabling", o, si estuviera publicado, con el "Addendum No. 5 of TIA/EIA-568-A".

Patch panel: Especificaciones de referencia:

- Todos los patch panel deben cumplir los lineamientos del FCC Parte 68, Sub apartado F, serán de 3.5" de alto proporcionarán 24/48 ports modulares RJ45, conexionados según la asignación de colores T568A/T568B.
- Los patch panels deben estar construidos de aluminio anodizado 0.118" de espesor con numeración clara y visible.
- Los patch panels deben estar configurados con 8 módulos de 6-port cada uno, reemplazables, con etiquetas universales con capacidad de codificación T568A y B. El frente de cada módulo será capaz de aceptar etiquetas de 9mm a 12mm y proporcionar para la misma un cobertor de policarbonato transparente. Cada port será capaz de aceptar un ícono para indicar su función.

- Los patch panels deberán cumplir con los requerimientos propuestos en la TIA/EIA-SP-4195, "Additional Transmission Performance Specifications for 4-Pair 100 Ohm Enhanced Category 5 Cabling", o, si estuviera publicado, con el Addendum No. 5 of TIA/EIA-568-A. Los patch panels deben estar validados por UL bajo el número E81956.

8.4 Subsistemas de Cableado vertical o de Backbone

Los cables del cableado vertical o del cableado de backbone (cableados entre racks principales, o entre racks principales y secundarios), deben ser UTP Cat6 (o superior) de 24 AWG, valuación UL/NEC CMR.

En los casos donde los backbone's verticales superen los 90 metros de distancia, se planteará una conexión física empleando cableado de fibra óptica. Las alternativas de fibra óptica a determinar por la Dirección General de Teleocmunicaciones según requerimientos, serán del tipo:

- **1 Gigabit Ethernet multimodo:** El cableado vertical se construirá con fibra óptica multimodo para Gigabit Ethernet (1000BaseSX), según las especificaciones de cableado en fibra óptica EIA/TIA 568-B.3.
- **1 Gigabit Ethernet monomodo:** El cableado vertical se construirá con fibra óptica monomodo para Gigabit Ethernet (1000BaseLX), según las especificaciones de cableado en fibra óptica EIA/TIA 568- B.3.
- **Gigabit Ethernet multimodo:** El cableado vertical se construirá con fibra óptica multimodo para 10 Gigabit Ethernet (10Base-SR/LX4), según las especificaciones de cableado en fibra óptica EIA/TIA 568- B.3.
- **Gigabit Ethernet monomodo:** El cableado vertical se construirá con fibra óptica monomodo para 10 Gigabit Ethernet (10Base-LX4/LR), según las especificaciones de cableado en fibra óptica EIA/TIA 568- B.3.

Especificaciones para fibras ópticas: Los cables estarán compuestos de un mínimo de 4 fibras ópticas. Especificación de referencia: Núcleo de 50 micrómetros y corona de 125 micrómetros con pérdidas no superiores a 3.5 dB/km.

Cada fibra óptica individual debe ser terminada en sus dos extremos con sus respectivos conectores. Especificación de referencia: Conectores metálicos con ferrule cerámico y estarán provistos de cubierta contra polvo y dispositivo eliminador de tensiones. Los conectores, el material de curado, los dispositivos necesarios para el curado y los acopladores para los empalmes de conectores deberán ser de la misma marca.

Los cables de fibra óptica se conectarán, en cada armario de distribución, a una caja de interconexión de fibras (Patch-enclosures) con capacidad para fijar y empalmar hasta 8 fibras individuales mediante los empalmadores correspondientes. Se deberá respetar rigurosamente el radio mínimo de curvatura especificado por el fabricante de la fibra, debiendo cumplir como mínimo con lo establecido por la norma EIA/TIA 568B.3, esto es radio

de curvatura mínimo de 25 mm para tendidos no tensionados y de 50 mm para tendidos bajo tensiones de hasta 220N.

Los cables UTP correspondientes a backbones o cableado vertical, se terminarán en patch panell en los racks (tal se menciona en la sección del subsistema de cableado de racks).

Instalación del Cableado vertical o de Backbone: Los cables del cableado vertical o de Backbone se instalarán de la manera siguiente:

- Los cables del cableado vertical o de backbone se instalarán en forma separada de los cables de la distribución horizontal.
- En el caso que se alojen cables de cableado vertical o de backbone en canalizaciones, los cables de distribución horizontal se instalarán en canalizaciones separadas.
- Donde se instalen cables de cableado vertical o de backbone, y cables de distribución horizontal, en una bandeja, se instalarán primero los cables de backbone y se sujetarán separadamente de los cables de la distribución horizontal.

8.5 Subsistema de Cableado horizontal

El sistema de cableado horizontal se extiende entre las áreas de trabajo (donde se encuentran los puestos de trabajo) y los racks secundarios (o de distribución).

Desde los racks secundarios o de distribución, se accederá a cada puesto de trabajo con dos cables de red.

Los cables de red del cableado horizontal deben ser del Tipo UTP (cuatro pares trenzados sin blindaje) categoría 5e (Enhanced Category 5) o superior. Alternativamente, y en forma justificada, puede recurrirse a cable del tipo FTP (cuatro pares trenzados con blindaje de hoja metálica), categoría 5e o superior, cuando cuestiones de ruido o interferencia lo hagan necesario.

La certificación del cableado horizontal se debe hacer según categoría 5e, bajo las especificaciones EIA/TIA 568-B (o su sucesora EIA/TIA 568-C).

Especificaciones de referencia:

- Debe ser 24 AWG, 4-pair UTP, UL/NEC CMR, con vaina de PVC.
- El cable debe cumplir con los requerimientos de la TIA Cat 5e en lo que a impedancia y atenuación respecta y excederá los valores NEXT Cat 5 del peor par en 6 dB.
- El cable debe ser exclusivamente de configuración geométrica circular y no se permiten soluciones implementadas con cables con geometrías de tipo ovalado llano, ni geometrías crecientes.
- El cable se debe se proporcionar en cajas de 300 metros y debe estar listado en UL (certificación emitida por Underwriters Laboratories).

021

Los cables de datos horizontales se terminarán en Patch Panels Enhanced Category 5 para montaje en bastidor de 19". Los circuitos de datos horizontales se conectarán a la electrónica de LAN dentro de cada rack.

Los circuitos de voz horizontales se conectarán a los Patch Panels que actuarán como espejo del repartidor dentro de cada rack secundario.

El tendido del cableado deberá ser realizado con las protecciones extras necesarias en cualquier sector del recorrido que pudiese significar un potencial daño en el cableado, por ejemplo, en la salida del rack, accesos a cajas de conexión y de paso, cruces de paredes, mamparas, etc.

Cuando el tendido del cableado de red es paralelo al de la distribución eléctrica, esta se hará por otro ducto, paralelo al que conduce la red de comunicaciones, y separado de éste por una distancia no menor a 25 cm, excepto en el caso de que se utilicen ductos metálicos conectados a tierra para su conducción, caso en el que la distancia podrá ser menor.

Consideraciones sobre la Instalación de Cable de Distribución horizontal:

- El cable se instalará de acuerdo con las recomendaciones del fabricante y las mejores prácticas de instalación de la industria.
- Desde cada rack saldrán las canalizaciones, las que deben ser estructuradas.
- La ocupación de las canalizaciones troncales y de distribución no deben superar el 70 % de su sección (capacidad) disponible.
- Los cables se instalarán en tendidos continuos desde el origen al destino y no se admitirán puntos de conexión adicionales intermedios a menos que específicamente se indique lo contrario.
- En el caso en que se permita la utilización de puntos de conexión adicionales intermedios, ellos se ubicarán en lugares de fácil acceso y en un bastidor pensado y conveniente para tal fin.
- Los cables UTP se deben instalar de forma tal que el cableado no presente cambios de dirección (en esquinas o curvas) que transgreda el radio de curvatura de mínimo. Se deben respetar los radios de curvatura según lo establecido por la normativa vigente EIA/TIA 568-B/C, a saber: Los cambios de dirección no deben presentar curvaturas menores a "cuatro veces el diámetro exterior de los cables" en ningún punto del recorrido.
- Los cables UTP se deben instalar de forma tal que en ninguna parte de su recorrido el cableado tenga tensiones mecánicas que excedan a las realizadas por 25 libras (11,3 Kg aproximadamente) para un solo cable o atadura de cables.
- Los cables de distribución horizontales no podrán agruparse en grupos de más de 40 cables. Las ataduras de más de 40 cables pueden causar deformación de los cables del centro de la atadura.

- No se precintarán cables a las grillas del techo suspendido o a los alambres de soporte de las luminarias.
- Cualquier cable dañado o excediendo los parámetros de instalación recomendados durante su tendido debe ser reemplazado por el proveedor de la instalación previo a la aceptación final sin costo alguno para la Municipalidad de Córdoba.
- Los cables serán identificados por una etiqueta. La etiqueta del cable se aplicará al cable detrás del faceplate en una sección de cable que pueda ser accedida quitando el Faceplate.

8.6 Subsistema de Cableado de oficina o planta

Se deben instalar en cada puesto de usuario, como configuración normal, una toma con dos circuitos de datos. Los dos circuitos de datos en cada toma se proporcionan vía dos cables Cat5e (Enhanced Category 5):

- Para aquellos puestos de trabajo que se encuentren sobre la pared (escritorios apoyados sobre la pared) se deben instalar, fijados a la pared, rosetas dobles para Jack RJ-45 Cat5e (o superior) o periscopios con dos Jack-RJ45 Cat5e (o superior).
- Para aquellos puestos de trabajo que se encuentren instalados en islas de trabajo separados de las paredes, se deben instalar periscopios. Estos deben contar con dos Jack-RJ45 por escritorios Cat5e (o superior).

El tendido de los cables dentro de oficinas y plantas de puestos de trabajo, hasta las tomas de conexión (rosetas o periscopios), a las cuáles se conectan finalmente los puestos de trabajo, se realizará a través de ductos (no se aceptan cables en cuyo recorrido estén desprotegidos). Si los mismos están tendidos sobre paredes, se debe colocar cablecanal. Si los mismos están tendidos sobre el suelo, se debe colocar piso canal:

- En aquellas ubicaciones donde no se transite frecuentemente: Piso canal de plástico.
- En aquellas ubicaciones donde exista paso de personas u otros movimientos: Piso canal metálico (de chapa o aluminio o similar).

Se deben prever todos los patch cord (uno por port) necesarios para conectar los puestos de trabajo de datos y de telefonía a las cajas de conexión (rosetas o periscopios). Estos serán patch cord Enhanced Category 5 de 8 pies (2,4 m). Los patch cords deben ser ensamblados y testeados en fábrica por el fabricante del sistema de cableado.

Todos los puestos de trabajo deberán ser etiquetados con indicación de número de puesto y función.

Tomas de Datos: Las tomas de oficina deben ser implementada mediante bastidores del tipo 110 Connect fase plates RJ45 (no se acepta que el mismo cable desde el rack termine conectado a un equipo de usuario). Cada toma de datos conectará dos cables Cat5e provenientes de un rack secundario (o de distribución). Cada cable se terminará en un

conector modular hembra RJ45 Enhanced Category 5 (8 posiciones/conductores) de acuerdo al código de colores T568A/T568B.

En el supuesto caso que sea necesaria la utilización de una caja de montaje superficial, cada caja de montaje superficial contendrá dos jacks modulares Enhanced Category 5 para datos. En esta terminarán dos cables Cat5e para cada puesto (como se indicó anteriormente).

Sea la toma un bastidor del tipo 110 Connect fase plates RJ45 o una caja de montaje superficial, deberán tener la capacidad de acomodar dos etiquetas y proporcionar un cobertor de policarbonato transparente para las mismas. A cada port se le proporcionará un icono para indicar su función.

Instalación de Toma de datos: Todas las tomas de datos se deben instalar de la manera siguiente:

- El exceso de cable se debe enrollar en las cajas de distribución o en las cajas de montaje superficial, teniendo presente que al alojar el rollo del cable no se debe exceder la especificación de los radios de curvatura.

Además, cada tipo del cable se debe terminar tal como se indica debajo:

- Los cables se deben terminar de acuerdo con las recomendaciones hechas en la TIA/EIA-568-A y/o las recomendaciones del fabricante y/o mejores prácticas de instalación de la industria.
- El destrenzado de los pares de los cables Cat5e en el área de terminación será el mínimo posible y en ningún caso será superior a media pulgada (12,7 mm).
- Los radios de curvatura de los cables en el área de realización de la terminación no serán menores a 4 veces el diámetro externo del cable.
- La vaina del cable se mantendrá tan cerca como sea posible del punto de terminación.
- Los jacks modulares RJ45 de datos ocuparán las posiciones superiores del faceplates. Los jack modulares de datos ubicados en faceplates orientados en forma horizontal o en las cajas de montaje superficial ocuparán la posición más a la izquierda disponible.

8.7 Testeo del Sistema de Cableado

Todos los cables y materiales de terminación deben ser 100% testeados de defectos en la instalación y para verificar la performance del cable bajo las condiciones de instalación.

Todos los conductores de cada cable instalado deben ser verificados por el proveedor previo a la aceptación del sistema.

Cualquier defecto en el sistema de cableado, incluyendo, pero no limitado a, conectores, couplers, patch panels y bloques de conexionado, debe ser reparado o cambiado para asegurar un 100% de utilidad de todos los conductores de todos los cables instalados.

Todos los cables deben ser testeados de acuerdo a las mejores prácticas de instalación. Si hubiera conflictos entre algunos de estos puntos, el responsable de la obra deberá llevar cualquier discrepancia a los líderes de proyecto para su clarificación y/o resolución.

En cada cable debe verificarse la continuidad en todos sus pares y conductores. Para los cables UTP de voz y de datos debe verificarse continuidad, pares reversos, cortos y extremos abiertos utilizando un tester tipo secuenciador. Además del testeo anteriormente citado, estos cables deben verificarse utilizando un analizador de cables.

Continuidad: Cada par de cada cable instalado debe ser verificado utilizando un secuenciador que verifique cortos, extremos abiertos, polaridad y pares reversos. A los cables del tipo mallado y apantallado se deben verificar con un tester que verifique la malla y/o pantalla de acuerdo a los lineamientos anteriormente descriptos. La verificación debe ser almacenada tipo pass/fail de acuerdo con los procedimientos indicados por los fabricantes, y referenciados a la identificación indicada en cada cable y/o número de circuito o par correspondiente. Cualquier falla en el cableado debe ser corregida y verificada nuevamente antes de su aceptación final.

Longitud: A cada cable instalado se le debe verificar su longitud utilizando un TDR (Time Domain Reflectometer). El cable debe ser verificado desde patch panel a patch panel, block a block, patch panel a Modular jack RJ45. La longitud del cable deberá respetar la máxima distancia establecida por el standard TIA/EIA-568-A. El largo del mismo deberá ser grabado con la identificación indicada en cada cable y/o número de circuito o par correspondiente. Para cables multipares la distancia del cable será la distancia del par más largo.

Verificación de la Performance: El cableado categoría 6 deben ser verificados utilizando un testeo del tipo automático. Este equipo de medición debe ser capaz de verificar los parámetros anteriormente descriptos como continuidad y longitud, además de esto debe proveer los siguientes resultados:

- Near End Crosstalk (NEXT).
- Attenuation.
- Ambient Noise.
- Attenuation to Crosstalk Ratio (ACR).

El resultado del testeo debe ser evaluado en forma automática por el tester, utilizando el último criterio del standard TIA/EIA (incluyendo de ser posible los requerimientos del Addendum Enhanced Category 5) y si es posible que el resultado mostrado sea del tipo pass/fail. El resultado debe ser bajado directamente desde el tester hacia un archivo, utilizando la aplicación del fabricante del mismo. Dicho resultado debe incluir todos los parámetros de testeo indicados.

8.8 Aterramiento y anclaje

La acometida (punto de entrada) debe estar equipada con un cuarto de puesta a tierra (Telecomunications Bonding Backbone, o TBB). Este Backbone debe ser usado para poner a tierra todos los cables mallados, equipamiento, racks, gabinetes, bandejas y otros equipos asociados que tengan un potencial asociado y que actúe como conductor. El TBB debe ser independientemente instalado de edificios eléctricos y de puesta a tierra, este mismo debe ser diseñado de acuerdo con las recomendaciones descriptas en el estándar TIA/EIA-607 (Grounding and Bonding).

El principal punto de entrada/cuarto de equipos en cada edificio debe ser equipado con una barra principal de tierra (TMGB). Cada cuarto de datos debe ser provisto con una barra de puesta a tierra (TGB). La TMGB debe estar conectada al punto de instalación de puesta a tierra del edificio. El propósito de este sistema es de proveer un sistema de puesta a tierra que tenga el mismo potencial al sistema eléctrico de puesta a tierra del edificio. La entrada principal en cada edificio debe estar equipada con una barra principal de aterramiento para datos (TMGB). La TMGB debe conectarse a la entrada de tierra del edificio.

El objetivo de este sistema es proveer un sistema de tierra cuyo potencial es igual a la tierra del edificio. De esta forma se minimizan las corrientes de fuga entre el equipo de datos y el sistema eléctrico al cual son conectados.

Especificaciones:

- Todos los racks, partes metálicas, mallas de cables, cajas, bandejas, etc., que se encuentran en los racks principales, deben conectarse a la respectiva barra de tierra TGB o TMGB usando como mínimo cable de tierra de #6 AWG y los conectores correspondientes.
- Si los paneles que se colocan en el rack no poseen suficiente superficie metálica de contacto para lograr una correcta puesta a tierra, entonces deberán vincularse al rack usando como mínimo cable de tierra de #14 AWG copper conductor.
- El tamaño del conductor de cobre debe seterminarse de acuerdo a la mayor potencia que alimenta cualquier equipo ubicado en el rack. El conductor debe ser continuo y conectarse en forma tipo daisy chain desde el extremo superior hasta el inferior anclado al rack usando los conectores correspondientes.
- Todos los cables de puesta a tierra deben identificarse con una aislación verde. Los cables sin aislación deberán identificarse con una cinta adhesiva verde en cada terminación. Todos los cables y barras de aterramiento deberán identificarse y etiquetarse de acuerdo a estándares.

Instalación del sistema de tierra

- La TBB debe ser diseñada y/o aprobada por un profesional calificado. La TBB debe seguir las recomendaciones de la TIA/EIA-607 standard, y debe instalarse de acuerdo con las mejores prácticas de la industria.

- La instalación y terminación del conductor principal de tierra hasta la tierra de la entrada del edificio, como mínimo, deberá ser ejecutada por una contratista eléctrica con licencia.

8.9 Sistema de Documentación y Entregables

La presente sección describe la instalación, administración, testeo y documentación requerida para la realización y/o mantenimiento al momento de la entrega de la obra.

Etiquetado: El instalador desarrollará y entregará un sistema de etiquetado para su aprobación. Como mínimo, el sistema de etiquetas debe identificar claramente todos los componentes del sistema: racks, cables, paneles y rosetas.

- Este sistema debe designar el origen y destino de los cables y una identificación única para cada uno de ellos dentro del sistema.
- Los racks y paneles deben etiquetarse para identificar su ubicación dentro del sistema de cableado.
- Toda la información sobre etiquetas debe documentarse junto con los planos o esquemas del edificio y todos los testeos deben reflejar el esquema de etiquetado utilizado.
- Todas las etiquetas deben imprimirse con tinta indeleble.
- Las etiquetas para los cables deben tener la dimensión apropiada según el diámetro externo del cable, y ubicarse de forma tal que puedan visualizarse en los puntos de terminación del cable en cada extremo.

Planos y/o esquemas: El instalador debe estar provisto con 2 juegos de planos tamaño D o E al comienzo del proyecto. Un juego estará designado como plano central para documentar toda la información que ocurra durante el proyecto. El juego central será actualizado por el instalador durante los días de instalación, y estará disponible un representante técnico durante el desarrollo del proyecto. Las variaciones durante el proyecto pueden ser los recorridos de cables y ubicación de los outlets. Al no haber variaciones, esto permitirá ubicar las terminaciones planeadas anteriormente de cables horizontales y de backbone o vertical, además de cables de puesta a tierra a menos que no sea aprobado por el propietario.

El encargado de obra debe proveer un juego del plano central al finalizar la obra. El plano realizado debe tener exactamente la ubicación de los puestos, ruteo de cables y el etiquetado del sistema de cableado. Además, será provista una descripción de las áreas donde se halla encontrado dificultad durante la instalación que pudieron causar problemas al sistema de datos.

Documentación de testeos: La documentación debe ser provista en una carpeta dentro de las tres semanas de haber finalizado el proyecto. Dicha carpeta debe estar claramente marcada con el título de "Resultados de Testeos".

Dentro de las secciones de backbone y de cableado horizontal se deben colocar los resultados de los testeos.

Dentro de la documentación se debe presentar el etiquetado del equipamiento, fabricante, número de modelo y la calibración más reciente por el fabricante. A menos que una calibración reciente sea especificada por el fabricante, y una calibración anual sea anticipada sobre todo el equipamiento de testeo utilizado en esta instalación. La documentación del testeo debe detallar el método de testeo utilizado y la configuración del equipamiento durante el modo de prueba.

Los resultados deben ser impresos en hojas del tamaño tipo A4. Esto debe ser agregado a la carpeta anteriormente descripta. Cuando se realiza una reparación y un re-testeo, se debe colocar ambos testeos Pass/Fail en la carpeta anteriormente descripta.

9. Sistema Switches de acceso

El presente apartado brinda las especificaciones técnicas mínimas para la provisión de switches de acceso. Especificaciones de referencia:

- 24 puertos 10/100/1000 de cobre. Autosensing para la Capacidad y Modo de Operación: Half y Full Duplex.
- Capacidad de al menos 2 y no más de 4 slots para instalar módulos con puertos de Fibra Óptica Gigabit Ethernet (1000 Base-Sx o Lx).
- Poder definir cualquiera de las vlans creadas como vlan de gestión o management.
- Poder definir interfaz IP en cualquiera de las vlans creadas en el equipo.
- Capacidad de Conmutación Capa 2 superior a 20 Gbps.
- Full Rate sin bloque en capa 2.
- Tasa de Conmutación de Tramas superior a 4 millones para tramas de 64 Bytes.
- Capacidad de Stacking superior a 1 Gbps Full Duplex.
- Cantidad de Direcciones MACs: 8000.
- Cantidad de Vlans: 4096.
- Soporte de Vlan por dirección MAC.
- Soporte de IEEE 802.1Q basado en puertos. Soporte Protocolo Trunking (IEEE 802.1Q).
- Priorización de Trafico: 8 niveles. IEEE 802.1p (Clase de Servicio/Calidad de Servicio) para entrada y salida de tramas.

- Control de Flujo IEEE 802.3x.
- Protocolo de Control de Agregación de Enlaces IEEE 802.3ad (puertos 10/100/1000 solamente).
- Soporte de Spanning Tree Protocol (IEEE 802.1D) por VLAN, tanto localmente como en los puertos de Trunk (IEEE 802.1Q).
- Soporte de protocolo POWER OVER ETHERNET, IEEE 802.3af.
- Soporte de Enlaces Agregados, el cual permite varias puertas Ethernet actúen como un solo canal o troncal.
- Interfaces RJ-45 y SFP. (Según necesidad y requerimientos).
- Soporte superior a 30 Grupos Multicast.
- Control de tráfico multicast por port, utilizando protocolos IGMP.
- Soporte de Mirroring de Puertos 1 a 1 y de 1 a muchos.
- Configuración por línea de comando, telnet, SSH.
- Soporte de IEEE 802.1X.
- Definición de listas de acceso (ACL) mínimo capa 2.
- Definición de Calidad de Servicio (QoS).
- Soporte de SNMPv1, SNMPv2 y MIB I y II.
- Reportes de alarmas, estadísticas de errores por puerto, porcentaje de utilización de la CPU, soporte de ping.
- Soporte de logueo de mensajes y alertas a través de Syslog y SNMP-Traps.
- Realización de backup y restore de archivos de configuración y sistema operativo del equipamiento.
- Compatibilidad con módulos SFP genéricos.
- Posibilidad de configuración a través de puerto USB/Serial.

10. Sistema Switches de core / Concentrador

El presente apartado brinda las especificaciones técnicas mínimas para la provisión de switches de core y concentradores. Especificaciones de referencia:

- 24 puertos 10/100/1000 de cobre. Autosensing para la Capacidad y Modo de Operación: Half y Full Duplex.
- Capacidad de al menos 4 slots para instalar módulos con puertos de Fibra Óptica: Gigabit Ethernet 1000 Base-Sx o Lx.

- Capacidad de al menos 4 slots para instalar módulos con puertos de Fibra Óptica: 10GBASE-LR.
- Poder definir cualquiera de las vlans creadas como vlan de gestión o management.
- Poder definir interfaz IP en cualquiera de las vlans creadas en el equipo.
- Capacidad de Conmutación Capa 2 superior a a 56 Gbps. Sin Bloqueo.
- Full Rate sin bloque en capa 2.
- Tasa de Conmutación de Tramas superior a 4 millones para tramas de 64 Bytes.
- Capacidad de Stacking superior a 1 Gbps Full Duplex.
- Cantidad de Direcciones MACs: 8000.
- Cantidad de Vlans: 4096.
- Soporte de Vlan por dirección MAC.
- Soporte de IEEE 802.1Q basado en puertos. Soporte Protocolo Trunking(IEEE 802.1Q).
- Priorización de Trafico: 8 niveles. IEEE 802.1p (Clase de Servicio/Calidad de Servicio) para entrada y salida de tramas.
- Control de Flujo IEEE 802.3x.
- Protocolo de Control de Agregación de Enlaces IEEE 802.3ad (puertos 10/100/1000 solamente).
- Soporte de Spanning Tree Protocol (IEEE 802.1D) por VLAN, tanto localmente como en los puertos de Trunks(IEEE 802.1Q).
- Soporte de Enlaces Agregados, el cual permite varias puertas Ethernet actúen como un solo canal o troncal.
- Interfaces RJ-45 y SFP. (Según necesidad y requerimientos).
- Soporte superior a 30 Grupos Multicast.
- Control de tráfico multicast por port, utilizando protocolos IGMP.
- Soporte de Mirroring de Puertos 1 a 1 y de 1 a muchos.
- Configuración por línea de comando, telnet, SSH.
- Soporte de IEEE 802.1X.
- Definición de listas de acceso (ACL) mínimo capa 2.
- Definición de Calidad de Servicio (QoS).
- Soporte de SNMPv1, SNMPv2 y MIB I y II.
- Soporte de protocolo POWER OVER ETHERNET, IEEE 802.3af.

- Reportes de alarmas, estadísticas de errores por puerto, porcentaje de utilización de la CPU, soporte de ping.
- Soporte de logueo de mensajes y alertas a través de Syslog y SNMP-Traps.
- Realización de backup y restore de archivos de configuración y sistema operativo del equipamiento.
- Compatibilidad con módulos SFP genéricos.
- Posibilidad de configuración a través de puerto USB/Serial.

ING. GUSTAVO E. SARAVIA
Subsecretario de Infraestructura
Tecnológica y Conectividad
Secretaría Ciudad Inteligente
y Transformación Digital

021